In collaboration with
the Wharton Blockchain and Digital Asset Project

WORLD
ECONOMIC
FORUM

Decentralized Finance (DeFi) Policy-Maker Toolkit

WHITE PAPER

JUNE 2021

Cover: Gradienta, Unsplash – **Inside:** Getty Images, Unsplash

Contents

3 Foreword

4 Executive summary

5 1 What is DeFi?

6 1.1 Distinguishing characteristics

7 1.2 The DeFi architecture

10 1.3 DeFi service categories

12 2 Risks

14 2.1 Financial

15 2.2 Technical

16 2.3 Operational

18 2.4 Legal compliance

18 2.5 Emergent risks

20 3 Policy approaches

21 3.1 DeFi and financial regulation

22 3.2 Available policy tools

24 3.3 Decision tree

25 Conclusion

26 Appendix 1: Background assessment

28 Appendix 2: Stakeholder mapping tool

30 Appendix 3: Decentralization spectrum

31 Appendix 4: DeFi policy-maker canvas

34 Contributors

35 Acknowledgements

36 Endnotes

Foreword

Sumedha Deshmukh
Platform Curator,
Blockchain and Digital Assets,
World Economic Forum

Sheila Warren
Deputy Head, Centre
for the Fourth Industrial
Revolution; Member of
the Executive Committee,
World Economic Forum

Kevin Werbach
Professor of Legal Studies &
Business Ethics, and Director,
Blockchain and Digital Asset
Project, Wharton School,
University of Pennsylvania

Decentralized finance (DeFi) is an emerging and rapidly evolving area in the blockchain environment. Although examples of DeFi have existed for several years, there was a sudden upsurge of activity in 2020. In one year, the value of digital assets[1] locked in DeFi smart contracts grew by a factor of 18, from $670 million to $13 billion; the number of associated user wallets grew by a factor of 11, from 100,000 to 1.2 million; and the number of DeFi-related applications grew from 8 to more than 200.[2] This growth in turn has stimulated interest from both the private and public sectors.

DeFi aims to reconstruct and reimagine financial services on the foundations of distributed ledger technology, digital assets and smart contracts. As such, DeFi is a noteworthy sector of financial technology (fintech) activity.

However, serious questions remain:

- What, if any, are the distinctive aspects of DeFi? What distinguishes a DeFi service from a similar service based on traditional finance?

- What are the opportunities and potential benefits of DeFi? To whom will these benefits accrue – and who might be excluded or left behind?

- What are the risks – individual, organizational and systemic – of using DeFi? How do these risks apply to clients, markets, counterparties and beyond?

- Can DeFi become a significant alternative to traditional financial services? If so, will there be points of integration? If not, what if anything will DeFi represent in the market?

- What novel legal and policy questions does DeFi raise? How should policy-makers approach DeFi? What options exist for addressing these questions?

Notably, the DeFi space is relatively nascent and rapidly evolving, so the full scope of risks and potential for innovation remain to be seen – and there are unique challenges in regulating and creating policies for such a new and changing area. This report does not recommend any one single approach; instead, it is designed as a set of tools that can be applied in light of the legal contexts and policy positions of each jurisdiction, which may vary. In the appendices we offer a series of worksheets and other tools to assist with the evaluation of DeFi activities. A companion piece, *DeFi Beyond the Hype*, provides additional detail about the major DeFi service categories.

Our hope is that this resource will enable regulators and policy-makers to develop thoughtful approaches to DeFi, while helping industry participants understand and appreciate public-sector concerns. It is the result of an international collaboration among academics, legal practitioners, DeFi entrepreneurs, technologists and regulatory experts. It provides a solid foundation for understanding the major factors that should drive policy-making decisions.

Executive summary

Decentralized finance ("DeFi") is a broad term for financial services that build on top of the decentralized foundations of blockchain technology. The space has evolved since the 2015 launch of the Ethereum network, which laid the groundwork by implementing blockchain-based smart contracts.[3] There has been increased interest recently, paralleling the 2013 spike in bitcoin price and the 2017 boom in initial coin offerings.[4] As new DeFi services aspire to reinvent elements of financial services, and billions of dollars of digital assets are pledged to DeFi capital pools, policy-makers and regulators face significant challenges in balancing its risks and opportunities.

DeFi proponents say it can address challenges within the traditional financial system.[5,6] Open-source technology, economic rewards, programmable smart contracts and decentralized governance might offer greater efficiencies, opportunities for inclusion, rapid innovation and entirely new financial service arrangements.[7] On the other hand, DeFi raises considerations related to consumer protection, loss of funds, governance complexities, technical risk and systemic risk. Significant incidents involving technical failures and attacks on DeFi services have already occurred.[8] Moreover, questions remain about the actual extent of decentralization of some protocols – and associated risks, e.g. for manipulation – and whether DeFi is more than a risky new vehicle for speculation that may open the door to fraud and illicit activity.[9]

The purpose of this document is to highlight DeFi's distinguishing characteristics and opportunities while also calling attention to new and existing risks – including the scope, significance and challenges of the fast-growing DeFi ecosystem. Understanding DeFi business models and the full set of relationships underlying DeFi is crucial for an accurate risk assessment and nuanced policy-making.

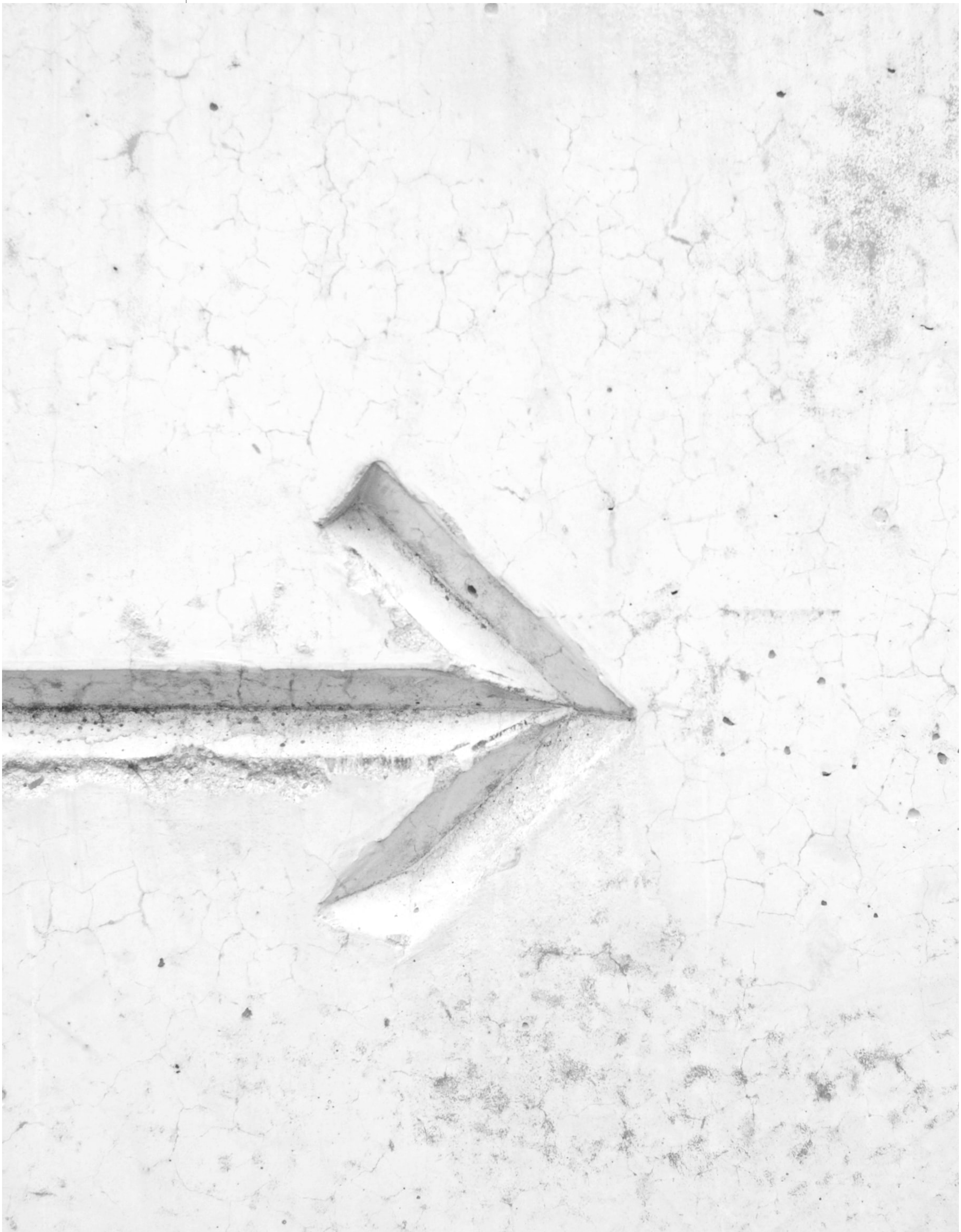
This toolkit:

- Provides an overview of the DeFi space generally, and the major classes of DeFi protocols, with tools to help understand the implications of new services
- Explores the potential benefits of the DeFi approach, along with the challenges that DeFi businesses will face
- Offers a detailed breakdown of the risks that DeFi may pose. Many of these are familiar concerns (although sometimes manifested differently), while others are unique to the decentralized, programmable and composable structure of DeFi
- Maps out potential legal and regulatory responses to DeFi

Our goal is not to recommend any specific actions universally, but to identify potential approaches and important considerations for the DeFi context. Financial regulatory regimes vary from jurisdiction to jurisdiction, as do policy-makers' judgements about the relative risks and rewards. DeFi will raise further questions about whether regulators have the proper tools to address evolving market activity, and how they can assert jurisdiction over a set of technologies and stakeholders that is intrinsically borderless and global.

Appendix 1 offers a background assessment for policy-makers and regulators looking to understand whether DeFi may be relevant to their entity. **Appendix 2** provides a stakeholder mapping tool for DeFi services. **Appendix 3** outlines the decentralization spectrum, while **Appendix 4** provides a DeFi policy-maker canvas.

1 What is DeFi?



"DeFi" is a general term for an evolving trend. Broadly, it is a category of blockchain-based decentralized applications (DApps) for financial services. DeFi encompasses a variety of technologies, business models and organizational structures,[10] generally replacing traditional forms of intermediation. DeFi transactions involve digital assets and generally operate on top of base-layer settlement platforms.

– **DeFi protocols** define software specifications and interfaces to create, manage and convert digital assets, building on a blockchain settlement layer.

– **DeFi services** implement DeFi protocols to create financial services, and associated functions such as specification of risk parameters and interest rates.[11]

– **DeFi users** access DeFi services to transact.

DeFi services may be made available to users through centralized web applications or permissionless interfaces such as programmable wallets or smart contracts. They may be provided by a traditional controlling entity, a community around a non-profit entity or a *decentralized autonomous organization (DAO)*, in which rights and obligations are specified in smart contracts.

1.1 Distinguishing characteristics

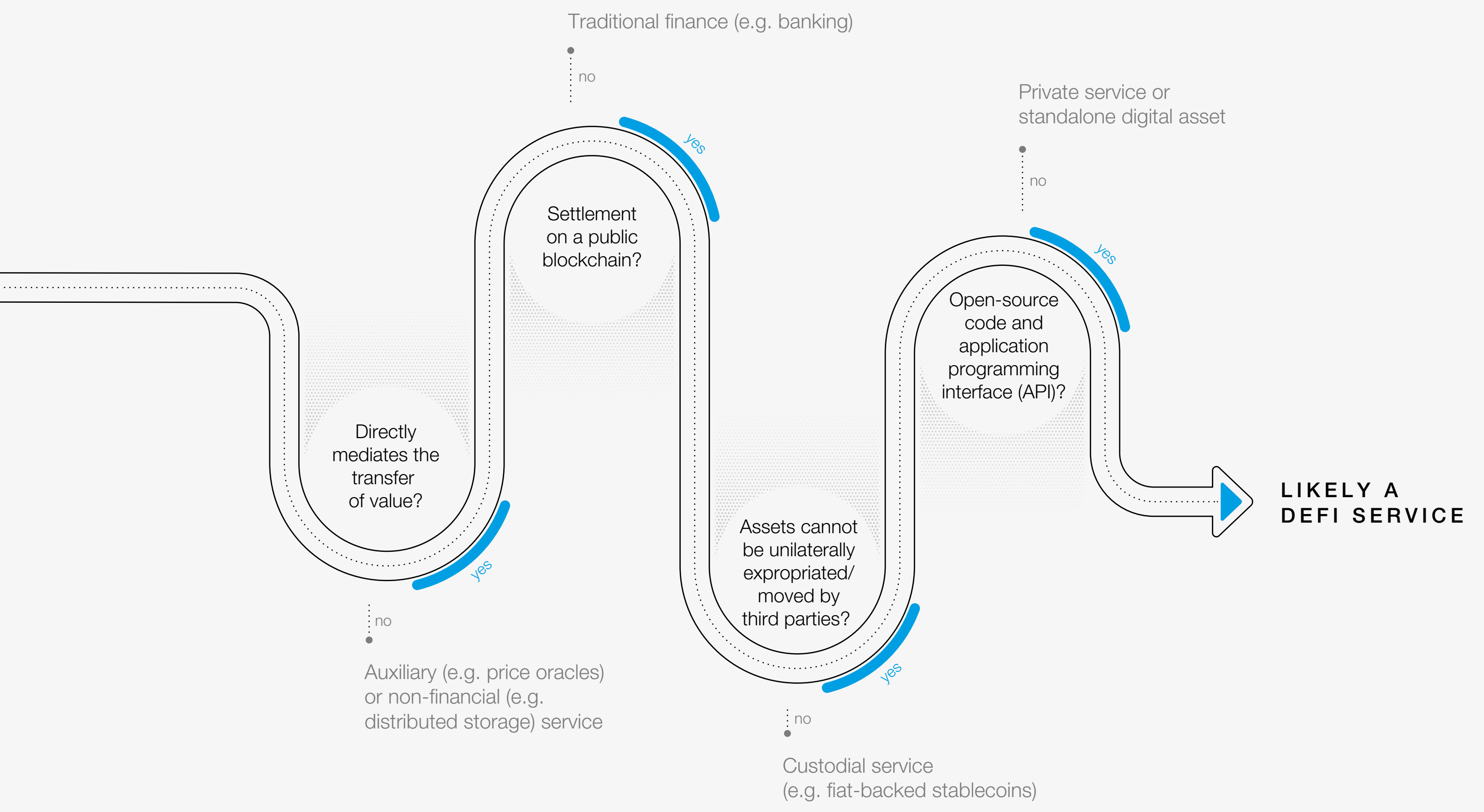
While the space is evolving quickly, we offer a functional description to distinguish DeFi from traditional financial services and auxiliary services. A DeFi protocol, service or business model has the following four characteristics:

1. **Financial services or products**
2. **Trust-minimized operation and settlement**
3. **Non-custodial design**
4. **Programmable, open and composable architecture**

Importantly, these characteristics represent the aspirations for DeFi. Businesses will exhibit each of these characteristics to varying degrees, and this may be fluid over projects' lifetimes.[12] Broadly speaking, the goal of DeFi solutions is to provide functions analogous to, and potentially beyond, those offered by traditional financial service providers, without reliance on central intermediaries or institutions.

Figure 1 provides a flow chart for evaluating whether an offering should be classified as DeFi.

FIGURE 1 **DeFi classification flow chart**


Traditional finance (e.g. banking)
no
yes
Settlement on a public blockchain?
Private service or standalone digital asset
no
yes
Open-source code and application programming interface (API)?
Directly mediates the transfer of value?
yes
no
Auxiliary (e.g. price oracles) or non-financial (e.g. distributed storage) service
Assets cannot be unilaterally expropriated/ moved by third parties?
yes
no
Custodial service (e.g. fiat-backed stablecoins)
LIKELY A DEFI SERVICE

1. **Financial services or products** means processing or directly enabling the transfer of value among parties. They are distinguished from information services, such as price feeds or storage, that only indirectly support value transfer.

2. **Trust-minimized operation and settlement** means that transactions are executed and recorded according to the explicit logic of a DeFi protocol's predetermined rules, on a permissionless basis. That is, due to their availability through a decentralized settlement layer, transactions do not require trust in the counterparty or a third-party intermediary. While the platforms vary, DeFi projects generally build on public, permissionless blockchains.[13] To date, most activity has been on the Ethereum blockchain, but activity is growing on other networks such as Algorand, Avalanche, Binance Smart Chain, Cosmos, EOS, NEAR, Polkadot, Solana and Tezos.[14]

   Service functionality is defined by a set of smart contracts. Both the settlement layer and the DeFi services have distinct governance structures – managed by one or more projects, communities or firms – that establish conditions for protocol changes. For example, a service may allow a volume of one token to be swapped for a corresponding volume of another token. This encompasses the price discovery, matching, execution and settlement functions of an exchange.

3. **Non-custodial design** means that the assets issued or managed by DeFi services cannot be unilaterally expropriated or altered by parties other than the account owner, even those providing intermediation and other services.[15] These tokens are subject only to the explicit logic of their smart contracts and the relevant DeFi protocols. Changes in those protocols, executed through the relevant governance structures, may affect the economic rights of digital asset holders.

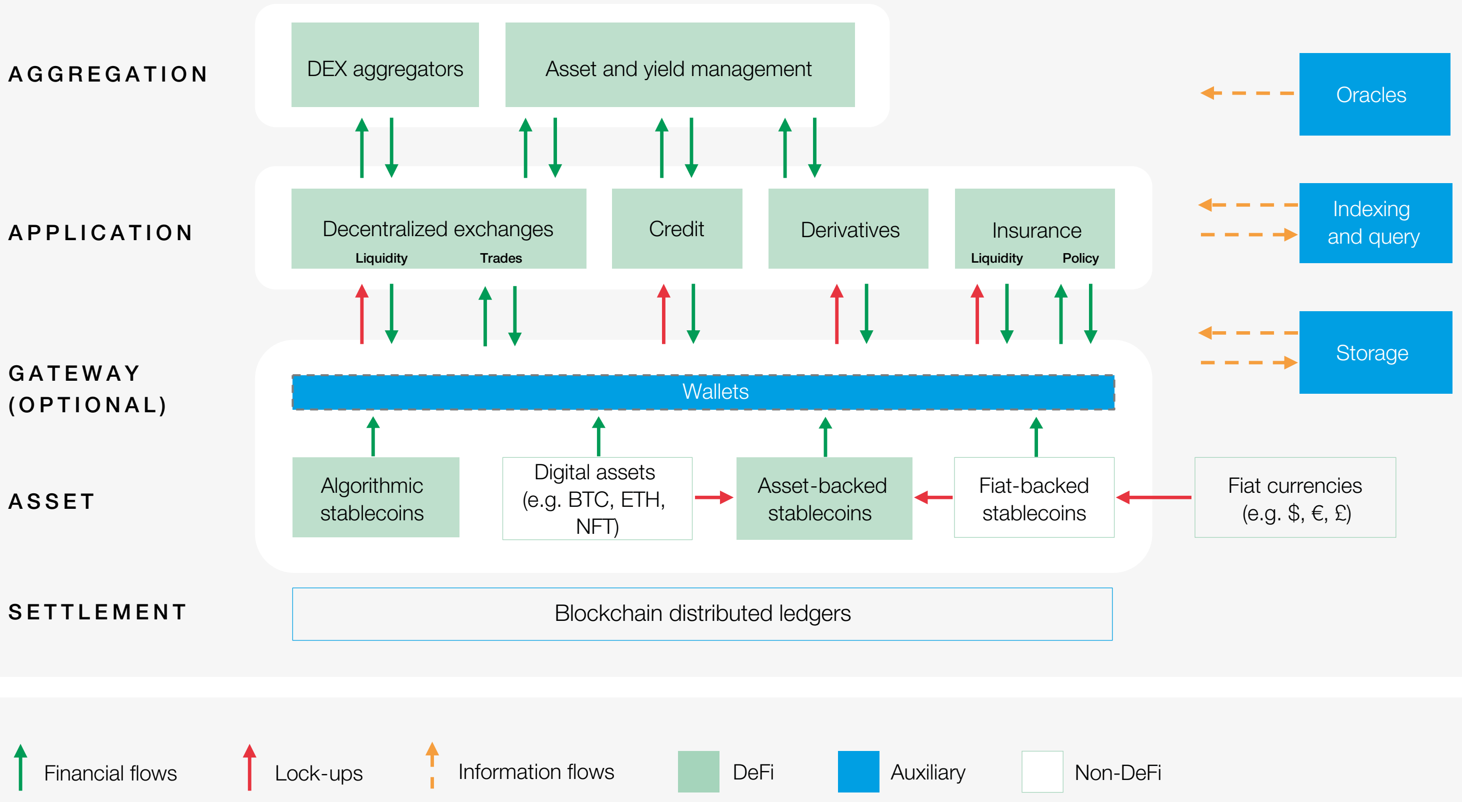
4. **Open, programmable and composable architecture** means that there is broad availability of the underlying source code for DeFi protocols and a public application programming interface (API) enabling service composability, similar to open banking[16] for centralized financial services. The widespread use of *open-source code* allows participants to view and verify protocols directly, and to fork code – take source code and create an independent development – or to create derivative or competitive services. The use of *open interfaces* means that third parties can understand, extend and verify the integrity and security of the service. Together with the API, this enables access to functionality in an automated, permissionless way. It also allows for *programmability*: customizing and extending financial instruments dynamically. For example, the terms of a derivative may be specified at the time of its creation, and then enforced immutably through the decentralized settlement layer.

   Composability means that these programmatic components can be combined to create financial instruments and services, including those incorporating multiple DeFi services and protocols. For example, a stablecoin may be used as the foundation for a derivative that is used as collateral on a loan and subject to an insurance contract. All of these services would be functionally interoperable, and the resulting instrument benefits from the common settlement layer of the underlying blockchain – but also faces common vulnerabilities.[17] As the number of DeFi service providers and available protocols grows and competition increases, specialization, interoperability and composability can enable growth in the connection between these services, and the economic activity between them.

1.2 The DeFi architecture

Figure 2 is a conceptual overview of the DeFi "stack".[18] The base-layer blockchain system enables participants to securely store, exchange and modify asset ownership information, replacing the *execution and settlement* layer of conventional financial services. It also allows for the creation of digital assets in various forms, which are then incorporated into DeFi *applications*. Additional layers of applications may function as *aggregators*, allowing users to shift among DeFi services, such as choosing an exchange based on real-time market factors. In this environment, digital assets may be transferred freely, based on contractual logic (financial flows) or they may be restricted from other uses to provide liquidity or collateral (lock-ups). There are also non-financial information flows that support the transaction activity.

FIGURE 2 | The DeFi stack



Information and content external to the blockchain may also be incorporated into DeFi transaction flows through *oracle* services, which supply reliable data that is recorded outside the settlement layer. For example, a price feed may draw on external data and be delivered programmatically through a smart contract. Such informational resources, as well as the wallet software and interfaces that help users store, transfer and manage assets interacting with DeFi services, are not themselves financial services and therefore we label them as *auxiliary* to DeFi.

Decentralized governance

Another dimension of the DeFi environment, not shown in Figure 2, is the implementation of decentralized governance mechanisms. Governance refers to the ways in which collective decisions are made, conflicts are resolved and changes to protocols are implemented. In DeFi, governance mediates activity between the applications and underlying settlement layer, including decisions such as altering interest rates or collateral requirements.

This new model raises several new questions for policy-makers and regulators, including:

- How are decisions made?
- How does accountability work?
- How does performance management work?

Many DeFi projects include a *governance token* that provides voting rights on certain governance decisions. Often these tokens are tradeable on exchanges, their value tied to scarcity and the activity level of the issuing DeFi service. Regulators will need to determine the appropriate classification of such tokens. It will be important to evaluate whether tokens are actually employed for governance or simply as a proxy for investment in the service.

FIGURE 3 | DeFi governance approaches

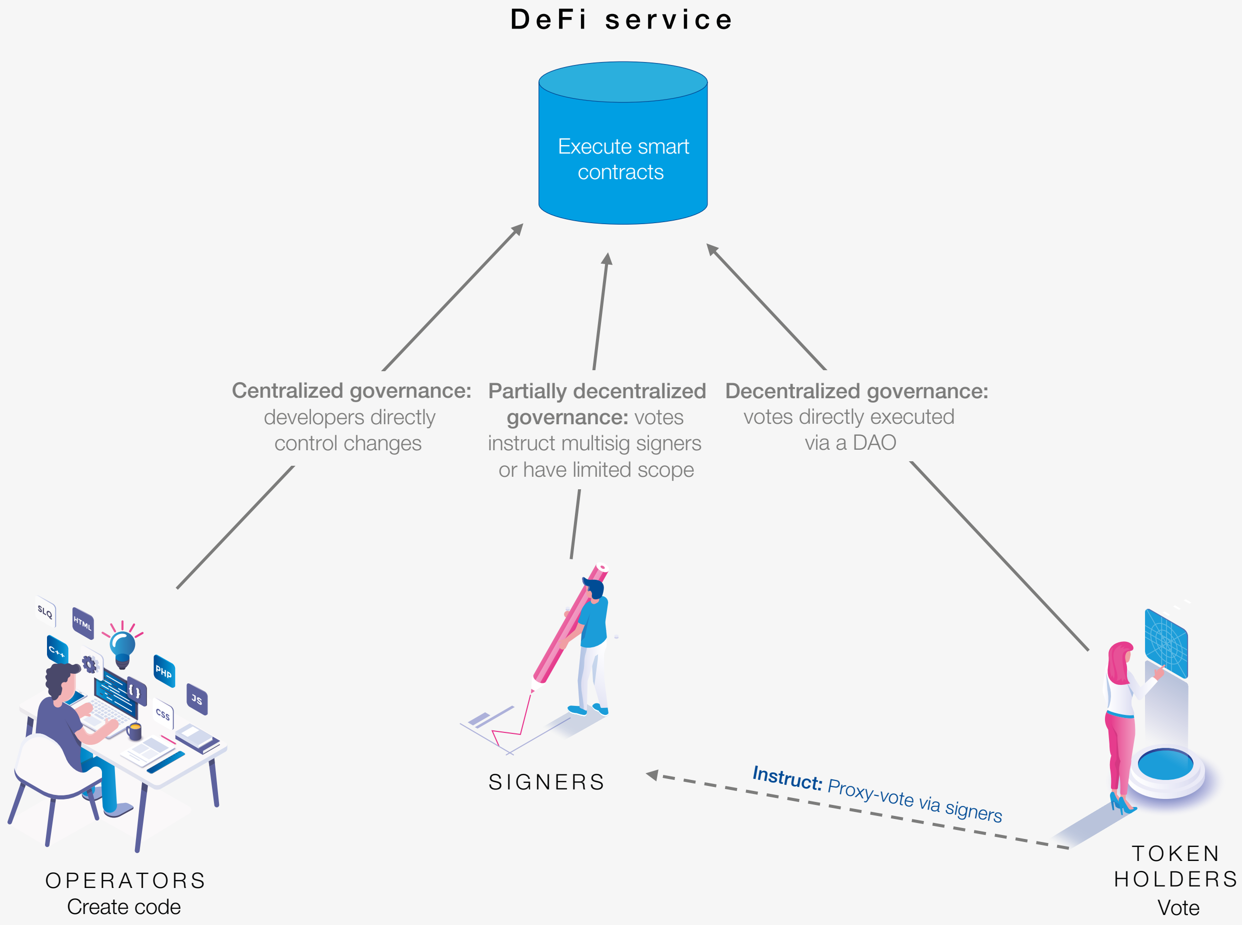

DeFi service
Execute smart contracts
Centralized governance: developers directly control changes
Partially decentralized governance: votes instruct multisig signers or have limited scope
Decentralized governance: votes directly executed via a DAO
SLQ
HTML
C++
PHP
JS
CSS
OPERATORS
Create code
SIGNERS
Instruct: Proxy-vote via signers
TOKEN HOLDERS
Vote

Figure 3 illustrates three forms of DeFi governance. The initial implementation is typically *centralized governance*, where the operator controls and implements changes directly.

Governance can be *partially decentralized* by giving token holders limited voting rights. They may have power over only a few parameters; developers may retain effective veto power through large token holdings or developers may have no formal obligation to implement proposed changes. In some instances of partial decentralization, individuals are designated to implement changes based on the instruction of token holder votes. They do so through *multisig keys*, wherein multiple signatures of delegates are needed to implement a change.

In *decentralized* governance, decisions move fully to a community of token holders through the establishment of a decentralized autonomous organization (DAO). DAO participants vote on changes to the protocol and are aligned through token incentives and rules written into smart contracts. Governance decisions are executed as blockchain transactions, enforced through the consensus mechanisms of the settlement layer.

DeFi developers often describe a trajectory from centralized governance at the outset to partially and then fully decentralized governance as the service reaches maturity. At this early stage of the market, however, there are few if any examples of this process unfolding from start to finish. The token-based voting systems that have been implemented are immature, and governance votes of major services have failed due to insufficient turnout.[19]

Token-based mechanisms for liquidity and governance expand the scope of interested parties beyond those in traditional financial services. Policy-makers should consider the implications of decisions on all of these stakeholder groups, and the incentives they create – especially considering: (1) who has control of the assets; and (2) who stands to benefit financially. **Appendix 2** provides a stakeholder mapping tool for DeFi services.

BOX 1 **DeFi incentive systems**

Many DeFi services incorporate explicit financial incentives to promote market development, including the creation of liquidity (for trading) and collateral (for credit):

- **Lock-up yields** pay interest or a share of trading fees for immobilizing digital assets to serve as liquidity or collateral for a service.
- **Liquidity mining** pays interest in the form of tokens issued by the service itself, typically governance tokens.
- **Airdrops** reward wallet addresses with tokens to promote awareness of new digital assets.
- **Yield farming** optimizes returns from liquidity mining and lock-up yields by automatically moving funds among services.
- **Liquidation fees** pay market-makers a percentage of the value of under-collateralized loans that they successfully liquidate (though not necessarily automatically).

These mechanisms are not necessary components of DeFi but have become widely identified with it. However, they may also distort investor expectations, generating unsustainably high returns as new capital is flowing in and token values are appreciating.

1.3 DeFi service categories

Due to their programmability and composability, the possible configurations of DeFi services are nearly endless. However, certain core functions, analogous to those in centralized finance, can be identified. These labels are generic and not intended as regulatory classifications for jurisdictions in which the terms used have legal import. A companion report, DeFi Beyond the Hype, provides greater detail on each of these categories.

Stablecoins seek to maintain a constant value for tokens relative to some stable asset – most commonly the US dollar. The ability to avoid the volatility of non-stabilized cryptocurrency such as bitcoin and ether is one reason for the growth in DeFi.

Custodial stablecoins use holdings of fiat currency or high-quality liquid assets as a reserve. Though they may be used in DeFi, these stablecoins are not DeFi services themselves because they involve centralized trust and custody.

There are two forms of stablecoin that meet the DeFi requirements listed in **Figure 1**:

- *Asset-backed* stablecoins use smart contracts to aggregate and liquidate collateral in the form of digital assets.
- *Algorithmic* stablecoins attempt to maintain the peg through dynamic expansion and contraction of token supply.[20]

Exchanges allow customers to trade one digital asset for another. The assets involved may be stablecoins or floating-value tokens. Unlike centralized exchanges such as Coinbase or Binance, *decentralized exchange* (DEX) protocols are DeFi services because they do not take custody of user funds and may not control other aspects of the process such as order book management and matching. An important category of DEX protocols for DeFi are *automated market-makers* (AMM), where an algorithm continuously prices transactions based on orders and available liquidity, rather than matching through an order book.

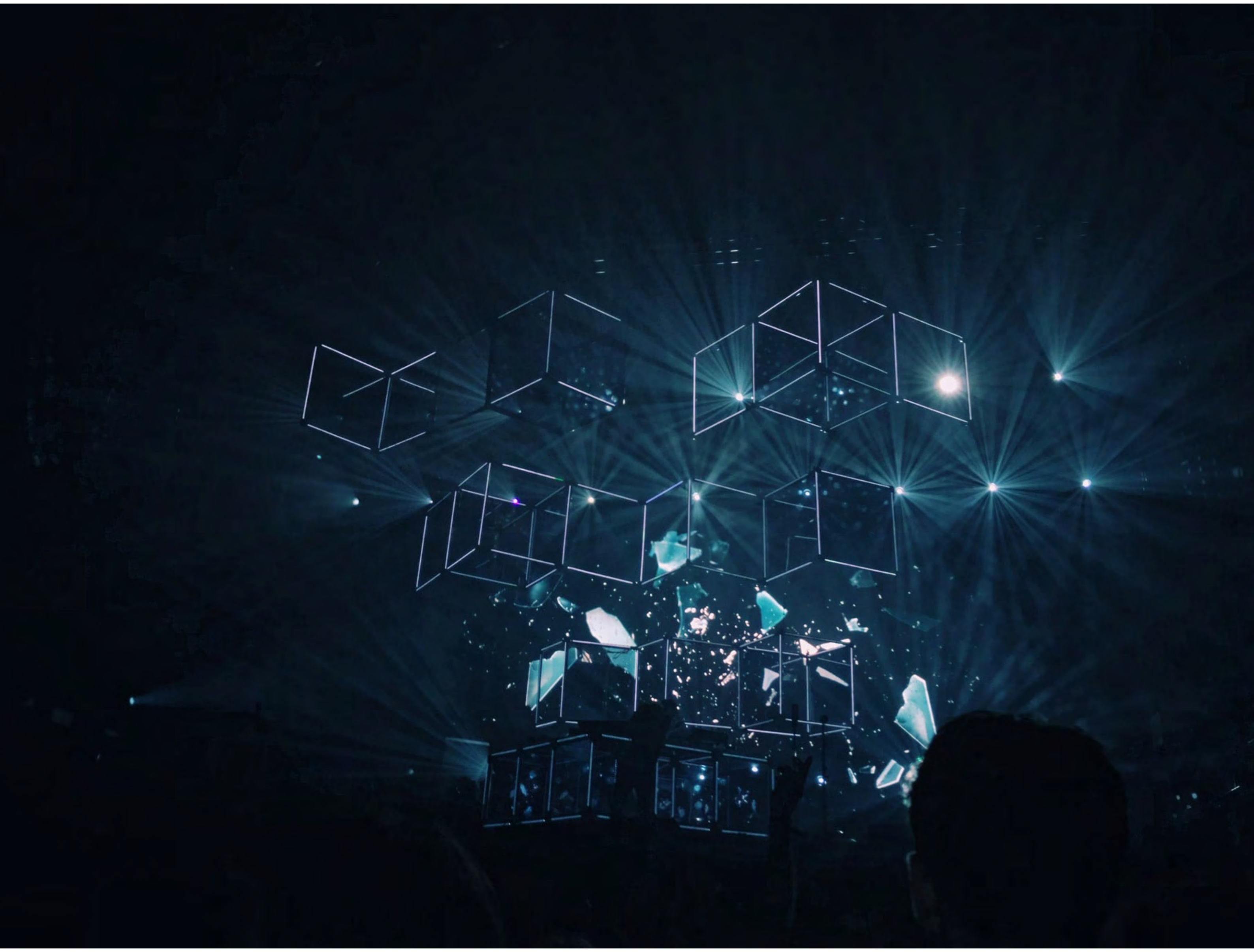
Credit[21] involves the creation of interest-bearing instruments that must be repaid at maturity. It is based on a mutual relationship of borrowers and lenders, which can be either bilateral (peer-to-peer) or based on pooled capital. Credit terms can be quite complex, and these instruments can themselves be securitized and traded. DeFi borrowing and lending replaces the intermediating function of financial service providers with automated, decentralized, non-custodial protocols. While the lack of credit ratings and legal recourse means that digital asset loans are nearly always over-collateralized, DeFi also allows for uncollateralized *flash loans* in which assets are borrowed and repaid (with interest) within the span of a single block's time.

Derivatives create synthetic financial assets whose value is reliant upon or derived from an underlying asset or group of assets. Common financial derivatives include futures and options, which pay out based on the value of an asset at some time in the future or deliver the underlying asset. DeFi derivatives can be programmed and composed into virtually any configuration. For example, a derivative could create a synthetic asset that behaves as a stock, commodity, swap or another digital asset. It could involve a non-fungible token (NFT) uniquely associated with an art or real estate asset. It might be tied to the activity of a business, creating a *crowdfunding* service. Or the value could be tied to a future real-world event, such as the outcome of a sporting event or political campaign, turning the derivatives exchange into a *prediction market*. Prediction markets may also incentivize decentralized information generation or dispute resolution through the wisdom of crowds.

Insurance pools risk by trading the payment of a guaranteed small premium for the possibility of collecting a large payout in the event of a covered scenario. In DeFi insurance, decentralized transactional and governance systems are used to manage and structure the insurance life cycle for certain types of risks such as smart contract hacks. Though technically insurance contracts are derivatives – they pay out based on some external event – insurance plays a distinctive risk-hedging function in markets by spreading risks across a common capital pool.[22]

Asset management involves the oversight of financial assets for others and seeks to maximize the value of the whole portfolio based on risk preferences, time horizons or other conditions. DeFi asset management promises greater transparency and efficiency in constructing and executing investment strategies, by incorporating the asset management life cycle into a DApp.

In addition, there are **auxiliary services** that support DeFi activity but are not themselves financial services. The most prominent are *oracles* (outlined above). Other auxiliary services include wallets, data storage, data queries, identity verification and arbitration.



2 Risks

This section provides a risk-mapping framework as a basis for policy considerations. It contains two stages: (1) identification of relevant risks; and (2) assessment of how DeFi market participants and others are addressing such risks.

We categorize DeFi risks into five categories (explored in more detail below):

Category	Associated risks
Financial Depletion of funds due to the transactional behaviour of fellow users concerning the digital assets in the DeFi service	Market risk
	Counterparty risk
	Liquidity risk
Technical Failures of the software systems supporting transaction execution, pricing and integrity	Transaction risk
	Smart contract risk
	Miner risk
	Oracle risk
Operational Failures of the human systems for key management, protocol development or governance	Routine maintenance and upgrades
	Forks
	Key management
	Governance mechanisms
	Redress of disputes
Legal compliance Use of DeFi to engage in illicit activity or to evade regulatory obligations	Financial crime
	Fraud and market manipulation
	Regulatory arbitrage
Emergent Macro-scale crashes or undermining of the financial system due to the interaction, scaling and integration of DeFi components	Dynamic interactions
	Flash crashes or price cascades

These categories are not mutually exclusive; some failures may result from multiple risks. There are also concerns inherent in the use of blockchains for settlement. For example, proof-of-work blockchains such as Bitcoin and Ethereum version 1.0 require computationally intensive mining, which raises concerns about energy usage that contributes to climate change. Because these issues are not unique to DeFi, they are beyond the scope of this report.[23]

Funds may be lost either unintentionally or due to deliberate attacks. Smart contracts do not distinguish intent and even undesired transactions may be effectively impossible to reverse. This problem was already evident in the 2016 draining of funds from the DAO,[24] the first DeFi service to accrue significant capital.[25] Finally, in some cases, the line between a legitimate trading strategy that takes advantage of an arbitrage opportunity and an improper exploit might be unclear.

2.1 Financial

Market risk is the possibility that asset value will decline over some time horizon due to market conditions, new information or traders' idiosyncratic behaviour. Though it may not be the role of governments to protect against market risk for well-informed and well-capitalized investors in a well-functioning market, it is appropriate for them to be concerned that those conditions are met. For DeFi, regulatory classifications will define whether requirements designed to prevent undue market risk – such as disclosure obligations and accredited investor standards – are applicable.

DeFi's novelty, as well as the ease of transferring funds and creating complex instruments, may increase the possibility of abuses, whether by the creators of DeFi protocols, the operators of exchanges or third-party manipulators. At the same time, policy-makers may want to consider the implications of potential increases in transparency as well as the retention of asset custody. There may also be a lack of observability and standardized price-discovery mechanisms found in digital asset markets. The inability to compare many of the current tokens to any fundamentals is a driver of big swings in valuation and overall volatility.

Counterparty risk is the possibility that a counterparty will default on its obligations to a financial instrument. This might involve failing to repay a loan (*credit risk*) or failing to settle a transaction by providing the specified asset (*settlement risk*). Though some credit risk is mitigated through interest rates for loans, it might be a particular problem in DeFi, where the volatility of underlying digital assets produces under-collateralization, the ease of credit creation leads to excessive leverage, or the algorithmic determination of interest produces inaccuracies. The lack of fixed identities in a pseudonymous network presents additional challenges in terms of determining creditworthiness. DeFi attempts to account for this through over-collateralization requirements.

Some traditional settlement risks are not present in DeFi because there is no separate settlement step; transactions are executed through transfer of the underlying value on the blockchain – but only if both sides of the transaction are operating on the same chain. Moreover, given the rapid inflow of capital, there are strong incentives and many opportunities for scams. Users may not receive the assets they anticipate due to fraud, especially when information asymmetries limit their understanding of investment decisions or the code that governs transaction execution.

Liquidity risk is the possibility that there will be insufficient funds or assets available to realize the value of a financial asset. Failure of liquidity for a borrower or trader (such as a short seller) means the position is involuntarily liquidated and the available assets allocated to owners or creditors. Insufficient liquidity also magnifies market inefficiencies, such as price movements resulting from trades.

DeFi liquidation processes differ from traditional instruments, where a centralized counterparty (a bank, the International Swaps and Derivates Association, a clearing house, etc.) executes the process. DeFi services often incentivize market-makers to liquidate under-collateralized loans, performing a function analogous to a foreclosure auction for real estate. If the liquidation incentive structures fail, however, original counterparties and liquidity providers hold unanticipated default risk. In DeFi markets where most transactions are automated and available continuously, the speed of liquidations may preclude rational decision-making. On centralized exchanges, cascades of automated liquidations have on several occasions produced "flash crashes", where prices dropped precipitously and trading was taken offline until the market settled. Such last-resort remedies may not be available for decentralized services.

DeFi liquidity risks may be mitigated through governance logic and the careful design of incentive structures. Game-theoretic analysis must anticipate not only expected behaviours, but other profitable strategies. For example, a market participant could deliberately skew liquidity in certain DeFi services and bet against the arbitrary results. Systems designed to incentivize stable liquidity could limit this risk. Because financial risks arise from profit-seeking, constant vigilance is needed to address new strategies.

Flash loans create a unique set of risks. They may effectively create artificial liquidity for a short period of time, seemingly addressing both counterparty and liquidity risk. If the loan cannot be paid back in time, the original transaction is never incorporated into the block and the loan is essentially rolled back before issuance. While flash loans may be used as near risk-free and low-cost capital for legitimate arbitrage transactions, they can also be employed in attacks. The temporary surge of funds can be used to manipulate prices and force artificial liquidation, often through the interaction of multiple DeFi services. Several million dollars have been stolen through several such high-profile, near-instantaneous attacks.[26]

2.2 Technical

According to Ciphertrace, half of digital asset hacks in 2020 targeted DeFi services, up from a negligible number in 2019 – a trend likely to continue as the value of assets involved grows.[27] While the largest public blockchain networks, such as Bitcoin and Ethereum, have avoided significant breaches, blockchain-based DApps and the centralized exchanges or wallets handling funds have proven far less secure. The technical complexity and immaturity of the DeFi market increases the likelihood of significant vulnerabilities, with the vast majority created in the past few years. The degree of interconnection among DeFi protocols may also expand the attack surface available to malicious actors.

Services aim to police market abuses through radical transparency and trust minimization rather than centralized oversight. Some include sophisticated, multilayered incentive structures to discourage attacks, in addition to technical measures for security and market integrity. Some have used their decentralized governance mechanisms to implement changes in response to failures or potential scenarios identified by the community. These measures are not foolproof. If DeFi continues to grow and attract less sophisticated market participants, investor protection concerns may grow.

Transaction risks are limitations or failures of the underlying blockchain network. If the base-layer settlement network is successfully attacked, allows for double-spending, becomes too expensive for transactions or lacks the necessary throughput, those failures will affect the application layer. The long-planned upgrade to Eth2 (Ethereum version 2.0), which aims for significant performance improvements, thus represents an important development for DeFi.[28] This upgrade will also shift Ethereum to proof-of-stake consensus, which does not require the intensive energy usage of proof-of-work mining.

Smart contract risks deal with code that does not execute as intended. All software has the potential for bugs. A programming flaw can cause a smart contract to fail to perform as desired, or attackers can exploit vulnerabilities to drain funds or engage in malicious activities. For example, where code has not been written properly, it can allow for exploits such as re-entrancy attacks. Complex software performing novel functions in a relatively untested environment, and often written by teams lacking the expertise or inclination to employ the most robust development practices, will tend to have more bugs than the norm.[29] Even without attacks, the smart contract might not accurately reflect the understanding of all parties. Because DeFi software is automated financial services, rather than a record-keeping mechanism subject to human override, coding errors can lead directly to financial losses, often without easy redress. Moreover, transparency of code has two sides – the visibility may make smart contracts more vulnerable to exploits or may offer opportunities for white hat hackers and bounty hunters to increase the robustness of the code.

CASE STUDY

The DAO exploit

The DAO, a decentralized crowdfunding platform, was arguably the first viable DeFi service. In 2016, ether then worth approximately $150 million was locked up in its smart contracts, with the goal of funding decentralized application development.[30] Before it launched, however, an attacker exploited a re-entrancy bug to drain approximately 40% of the funds into a "child DAO". To prevent permanent loss, and the collapse of confidence in Ethereum, miners agreed to implement a hard fork that reversed the theft on the main Ethereum chain. A minority faction continued mining the deprecated chain, which became known as Ethereum Classic.

Mechanisms such as security audits and bug bounties can be employed to mitigate smart contract risks. Over time, common errors in smart contracts written in popular languages such as Ethereum's Solidity become more familiar, and high-quality teams know to look for common attack vectors.

Miner risk deals with the possibility that transaction processing entities behave maliciously towards certain transactions. This depends on the correct ordering and execution of transactions sent to a DeFi smart contract. It operates at an analogous level to settlement risk in centralized finance, involving the finalization of transactions, although the nature of the threat is different. In blockchain systems, users typically send a transaction to the network along with a fee to the miner that successfully processes it into a block. Miners take proposed transactions and decide the order in which to execute them. However, a miner need not execute transactions in fee order. A miner can choose to execute a lower-fee transaction ahead of a higher-fee transaction, if that transaction is particularly valuable to them, or in return for a side payment from the originator of the lower-fee transaction.

Such behaviour allows for a form of market manipulation like front-running in high-frequency trading. By manipulating the order of execution, a miner can effectively allow certain parties to compound returns faster than others. Some view "miner extractable value" as inevitable in any system based on public blockchains, which is legitimate if structured transparently and fairly. This is a topic of active debate in the DeFi community.[31]

CASE STUDY

DEX arbitrage bots

Researchers have documented and quantified the rising deployment of arbitrage bots in decentralized exchanges.[32] Like high-frequency traders on Wall Street, these bots exploit inefficiencies, paying high transaction fees and optimizing network latency to front-run (anticipate and exploit) ordinary users' DEX trades. They study the breadth of DEX arbitrage bots in a subset of transactions that yield quantifiable revenue to these bots by engaging in priority gas auctions (PGAs), competitively bidding up transaction fees in order to obtain priority ordering, i.e. early block position and execution, for their transactions.

Oracle risk involves the potential that data external to the blockchain on which a DeFi contract relies is inaccurate or has been manipulated. Oracle-dependent DeFi protocols are susceptible to attacks in which oracle providers can manipulate the price observed on-chain. If on-chain asset holders can do this, they can increase the value of their on-chain asset or decrease the value of other participants' assets. Re-marking below a liquidation threshold could lead to assets being sold to the highest or first bidder.

If an oracle uses a centralized data source, such as a feed from CoinMarketCap for prices, this represents a source of centralized trust and vulnerability. An oracle can be decentralized by using multiple data sources or by incentivizing providers to submit data. Decentralization makes it difficult for a small number of participants to manipulate prices. On the other hand, payments to data providers must be designed effectively for fairness and incentive compatibility to ensure accurate information. Poor mechanism design may make it profitable to manipulate oracle data feeds. There have already been several successful DeFi oracle attacks.

CASE STUDY

The Compound oracle exploit

In November 2020, the price of the DAI stablecoin was temporarily driven up 30% over its $1 peg on the Coinbase exchange, which was used as the pricing oracle by the Compound DeFi credit platform.[33] When the DAI price spiked, it caused Compound's smart contracts to determine that many loans were under-collateralized. This triggered $89 million of assets locked in Compound to be liquidated automatically. It is unclear what caused the anomalous increase in the Coinbase price, but it could have been an intentional form of manipulation directed at Compound. This event illustrated the risks inherent in the interconnection among DeFi and other blockchain-based financial systems – and that some elements of the ecosystem may not be as decentralized, and therefore more vulnerable, than it initially appears.

2.3 Operational

Even though DeFi activity is highly automated, human operators still play a crucial role. The more decentralized a service, the less risk there is associated with any single point of failure. Auxiliary services may be centralized even when the DeFi service is highly decentralized. At the same time, greater decentralization can make it harder to respond effectively when something goes wrong. The fewer people who have unique power to break a service, the fewer who have the power to fix it.

Routine maintenance and upgrades may be more difficult to implement for decentralized services, or may create vulnerabilities, especially given the composability of DeFi. This would also include ongoing network and node connectivity and considerations related to security and cyber risks.

Code **forks** are options for groups seeking to alter elements of DeFi services, providing an "exit" option for minorities that prefer a different set of parameters.[34] In some cases, a fork may become more popular than the original service. When there is already significant activity on a platform, however, forks can be costly and confusing for participants. They can also be employed for malicious purposes, including to mislead users.

CASE STUDY

SushiSwap vampire attack on Uniswap

In September 2020, a pseudonymous developer, Chef Nomi, forked Uniswap, an open-source decentralized exchange, to make SushiSwap, a nearly identical exchange with an added token (SUSHI) and token rewards for liquidity providers and token holders.[35] The incident, which became known as the first "vampire mining" event, was unique in that SushiSwap indirectly competed with Uniswap by providing the same service using identical code but with an additional incentive, draining Uniswap's liquidity. Initial participants in SushiSwap earned SUSHI by depositing Uniswap's LP tokens, which represented user deposits in the Uniswap DEX. These Uniswap LP tokens were then swapped for the SUSHI, so that Uniswap liquidity would become SushiSwap liquidity. Ten days later, the pseudonymous developer sold all of his SUSHI tokens for $13 million in Ether and handed over control of the protocol to the Chief Executive Officer of FTX, a centralized exchange.

Key management is a potential problem for all blockchain-based systems. Platforms identify users and their assets through cryptographic key pairs. Because DeFi services are non-custodial, they place the key management burden on their users in return for removing dependencies on centralized service providers. A variety of techniques including requiring multiple signatures (multisig), social recovery and custody arrangements have been developed to address key management risks for digital assets.

Governance mechanisms for DeFi and other blockchain-based services raise complex potential risks. "One-token, one-vote" may be exploited when participation rates are low, token control is concentrated or participants can bribe each other to vote in their favour. Centralized exchanges may take advantage of the voting power of tokens in their custody to exert undue influence in governance. Specialized DeFi market participants may engage in activities analogous to activist investing, deliberately acquiring significant shares of governance tokens for a service. With enough voting power, these investors could change the parameters, allowing them to drain liquidity pools. Even though many of the mechanisms incorporated into DeFi governance systems have a history in academic literature, their behaviour with large numbers of participants and millions or billions of dollars at stake remains unproven. Moreover, a recent research paper presents evidence that DeFi token holdings are heavily concentrated, in ways that are not entirely transparent.[36]

CASE STUDY

Flash loans and MakerDAO governance

Flash loans also pose challenges for governance systems. In late October 2020, an attacker used a flash loan to acquire $7 million of the MKR governance token associated with the MakerDAO protocol and exercised its rights to vote on a governance proposal. Concerned about the potential for abuse, MakerDAO adopted restrictions shortly thereafter to prevent this scenario from being repeated, but other DeFi services remain vulnerable to such attacks.

Redress of disputes is a final category of governance risks. Once a smart contract has executed, the output cannot be modified or reversed just because an individual actor, or a governmental authority, orders it to be. When participants believe they are entitled to redress for some failure of the system or malicious act, arbitration may be incorporated into the DeFi service through multisig arrangements or be decentralized through a prediction market or crowdsourcing mechanism. However, these novel mechanisms have their own limitations, for instance, compared to judicial or administrative orders.

With a well-designed DeFi service, operational risks may be measured in real time and actively mitigated. DeFi transaction ledgers are public, so malicious activities may be tracked more easily than in analogous cases for centralized finance.

2.4 Legal compliance

DeFi may be used to bypass legal or regulatory obligations. The activities involved could occur with any service involving digital assets. Money laundering, for example, is a problem for established centralized cryptocurrency exchanges as well as DeFi DEXs. Because the focus of this report is on the distinctive challenges and opportunities of DeFi, we provide only a brief summary of risks in this category.

While a DeFi structure may not increase the likelihood of such violations *per se*, it could complicate enforcement. The decentralized, non-custodial, composable nature of DeFi services may make it difficult to identify a responsible party, for example. Regulatory regimes built around intermediaries as regulated processors of transaction information may fit poorly with a disintermediated market structure. We consider how regulators and policy-makers might address such challenges in Section 3, below.

Financial crime involves breach of anti-money laundering/countering the financing of terrorism (AML/CFT) restrictions, financial sanctions and similar legal regimes. DeFi transactions involving natively digital assets may be difficult to regulate through traditional AML/CFT controls because users are pseudonymous by default, transactions are resistant to blockage, assets are resistant to seizure and many transactions involve non-custodial wallets not directly tied to individuals. Although DeFi transactions are generally transparent and traceable, new privacy-enhancing protocols and/or tools may create additional regulatory challenges. Several approaches have been developed to comply with the 2019 anti-money laundering guidance for digital asset service providers from the Financial Action Task Force (FATF), but further work remains and could be further affected by new guidance proposed in March 2021 that could require know-your-customer (KYC) compliance from DeFi services.[37] In particular, the use of non-custodial arrangements and self-hosted wallets in DeFi poses a challenge for requirements that identifying metadata be collected and passed for every transaction link.

Fraud and market manipulation involve deliberate scams, misappropriation and other efforts to take advantage of investors. Here we refer to activities conducted or enabled by DeFi developers themselves, rather than third-party attacks. For example, "rug pulls" or exit scams involve convincing users to place funds into a seemingly legitimate DeFi service, from which they are drained by the developers, who then disappear.

Regulatory evasion means failing to meet regulatory obligations by carrying out similar functions in a different technical manner. It may involve deliberately obfuscating activity or masking the jurisdictional attributes of transactions. On the other hand, the fact that a novel activity bears similarities to an established one does not automatically imply regulatory arbitrage. Poorly designed regulatory obligations could themselves be viewed as a risk factor for DeFi. All major categories of DeFi activity can be viewed as alternatives to regulated financial services. Whether they are subject to similar classifications goes beyond the scope of this report, and the answers will vary by jurisdiction.

2.5 Emergent risks

Emergent risks involve the interaction effects of multiple events, creating failure cases that are not reflected in a risk assessment of each service independently. Classic recent examples are banks that are "too big to fail" and scenarios in which ostensibly unrelated events, such as individual mortgage defaults, become highly correlated and produce cascading effects through chains of securitization. Other examples include system-wide liquidity failure due to bank runs or markets "freezing up" when parties are unwilling to transact due to perceived risk.

Dynamic interactions among a potentially endless number of interconnected DeFi components may produce risks that are not present in any individual service. Also, because DeFi operates in a global market, activities are not necessarily limited to countries or business segments as they are when transactions are based on a national sovereign currency. Unless regulators can effectively limit cross-border DeFi activity, firebreaks to contagion of systemic defaults may be more limited than for traditional finance. Interaction risks will also grow as DeFi services begin to interoperate with traditional financial platforms.[38]

Flash crashes or price cascades, exacerbated by leverage in the DeFi system, may occur in extremely volatile or rough market conditions. Unlike traditional markets, where primary dealers and brokers can manually intervene when defaults occur concurrently, the permissionless, algorithmic nature of DeFi means that it may not be possible to stop cascades. DeFi services that automatically liquidate collateral allow liquidators to compete to buy that collateral, sometimes offering a fixed discount as an incentive. However, when a flash crash occurs or market volatility is high, there may be so many liquidations and the drop in the price of the collateral may be so precipitous that liquidators or others will face significant losses.

MakerDAO's Black Thursday

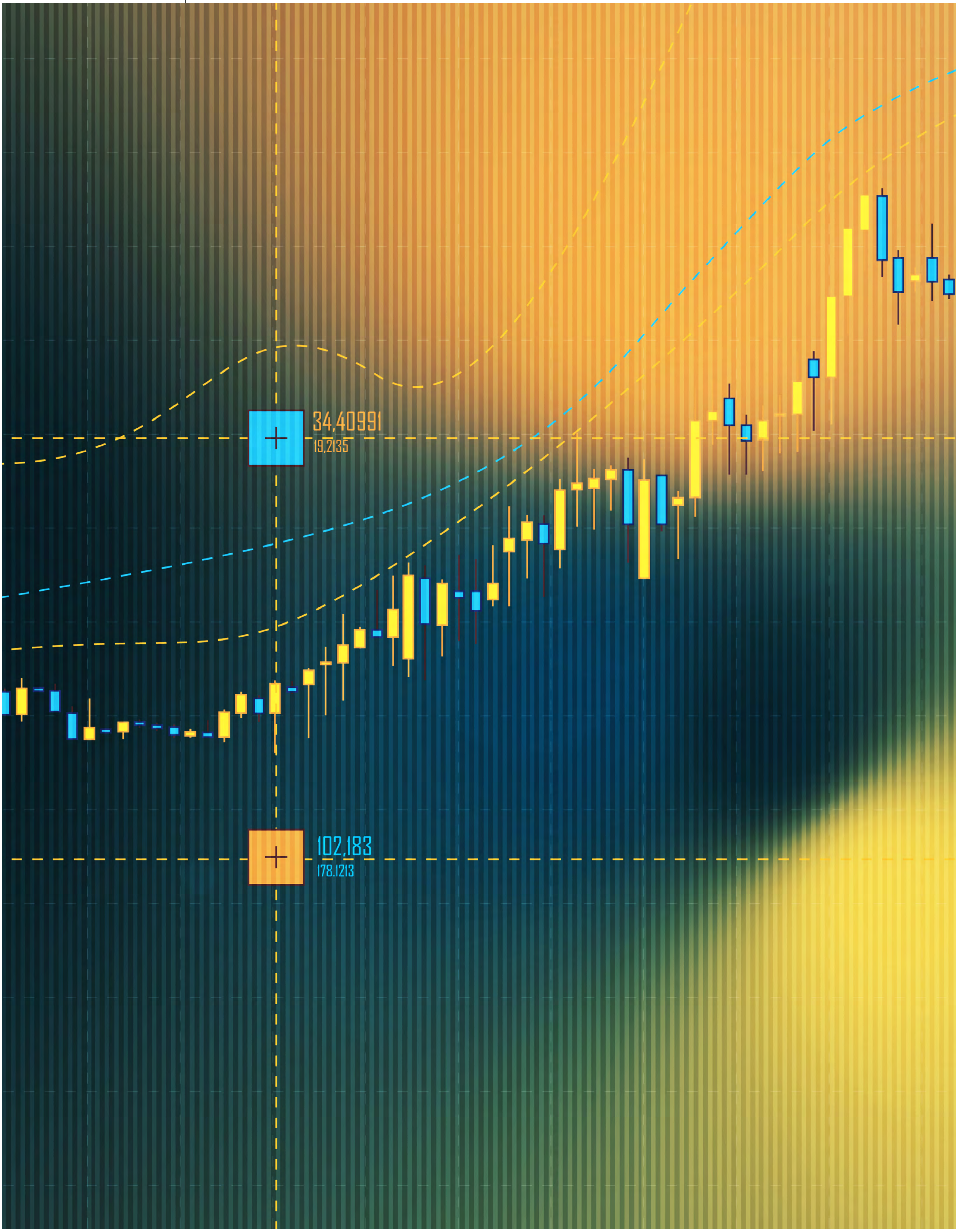
One of the largest systemic failures of a DeFi service took place on Thursday 12 March 2020, when Maker Protocol's liquidation system failed and more than $8 million in user assets was lost.[39] This was exacerbated by network congestion on the Ethereum blockchain, which increased "gas" prices for validating transactions and slowed the flow of data updates to MakerDAO's oracle service.

A class-action lawsuit over the event, claiming that the Maker Foundation deceived collateral providers by failing to appropriately disclose such risks, was sent to arbitration in September 2020. The event exposed emergent risks faced by the DeFi protocols, including the availability and reliability of the underlying blockchain infrastructure.

Assessing such risk is difficult. Most traditional financial models assume that liquidations always occur successfully, as the trusted third party (exchange, broker, dealer) will close a position when unprofitable. In DeFi, this is true only when liquidators can achieve a profitable liquidation. If cascades persist for too long, liquidators stop liquidating and traditional value-at-risk (VaR) models break down. This failure is akin to what happened during the 2008 financial crisis, when centralized third parties that enforced liquidations, such as AIG, failed.

Risks of this form can be estimated using tools such as agent-based simulation, which model rational behaviour for all principal parties (borrowers, lenders, traders and liquidators) and then run millions of event-based Monte Carlo simulations – models for predicting outcomes for situations subject to random variables – to estimate worst-case loss. Unlike traditional financial Monte Carlo simulations, these simulations explore conditions in which financial assumptions such as no-arbitrage and instant liquidation are invalid. Using such models, corrections to traditional value-at-risk (VAR) models can be estimated, leading to estimates of default probability as a function of parameters such as volatility.

3 Policy approaches



This section outlines the main areas in which DeFi may interact with policy and regulation. Importantly, it lays out key issues and options but does not offer prescriptive solutions, as jurisdictions vary in their objectives, regulatory regimes and market composition. The approaches described here are intended to be sufficiently generic to apply in the full range of contexts. The remainder of this section provides tools and resources.

Trust-minimized execution, non-custodial services and composable architectures may challenge the existing regulation. As described in Section 2, DeFi can both introduce new risks and may help mitigate known risks in financial services. Many of the key challenges for policy-makers – the way in which decentralization makes it difficult to identify regulatory subjects, new risks due to automation, and the way in which borderless software code complicates the application of territorial rules – are extensions of issues for all digital assets. Others, such as the creation of building blocks with multiple potential use cases and integrations, or the incentive structures of tokenized governance, are less familiar. Given the cross-cutting nature of DeFi, an integrated strategy and vision is needed.

Generally, it may be wise to consider a **technologically neutral** approach to balance meeting the objectives of regulatory regimes with promoting innovation and market development. As with any regulatory initiatives, policy-makers should strive for DeFi rules that are fair, efficient, effective and enforceable.

A policy-maker canvas, included as **Appendix 4**, is designed to apply key components of this section in a structured manner.

3.1 DeFi and financial regulation

The first step is to identify the relevant objectives and associated categories of policy and regulation. Common goals for financial regulation include: protection of investors and other consumers; market efficiency and integrity; capital formation; financial inclusion; prevention of illicit activity; safety and soundness; and financial stability. Each provides a distinctive logic for certain kinds of rules. For example, regulators focused on investor protection are typically concerned that custodians are not able to abscond with funds. The non-custodial nature of DeFi may alleviate some of these worries, while creating new ones (as outlined in Section 2).

DeFi activity spans many domains of financial regulation, including securities, derivatives, exchanges, investment management, bank supervision, financial crime, consumer finance, insurance, risk management and macroprudential oversight. A coherent overarching strategy is important and could be delegated to a cross-entity taskforce or similar body. Some DeFi activity patterns will clearly match established legal categories; others will not.

A range of policy actions may be adopted for DeFi, including:

- **Forbearance**: decision that no new regulations are needed
- **Warnings**: issuance of warning to users/consumers
- **Enforcement**: determinations that existing rules already cover the relevant actors and activities and have not been complied with
- **Opt-in**: provide the option to become subject to regulations in return for certain protections, even though there is no legal requirement
- **Pruning regulations**: eliminate regulatory requirements that are no longer essential in a DeFi context
- **Limited licence frameworks**: the possibility of obtaining licences of limited scope or under size thresholds, with light-touch requirements
- **Prohibitive measures**: prohibit certain activities in the DeFi sector
- **New licence types**: address risks with new categories designed for DeFi
- **Issuing guidance or expectations**: craft new frameworks, often with a public comment or consultation included before its official release

An effective regulatory response to DeFi is likely to involve a combination of existing regulation, retrofitted regulation and new, bespoke regulation.[40] An emerging body of digital asset-specific law is growing, including the European Union's comprehensive Markets in Crypto Assets (MiCA) proposal.[41] However, most jurisdictions are yet to adopt bespoke frameworks.

Most financial regulatory regimes focus on those "carrying on business" in a certain regulated activity, "dealing", "arranging" or "operating" some scheme or exchange or "issuing" an offer (or similar). Historically, the relevant government entity was relatively clear and focused on who is ultimately in control of an operation. Similarly, there are often exemptions for service providers that merely provide infrastructure, data or other tools to enable others to layer on their financial services. Frameworks contemplate definable and centralized operators that are engaged in providing particular financial end products and services, but are not necessarily the underlying builders.

In the DeFi context, however, there may be no central entity performing the relevant activities. The software developers and token holders may be easily identifiable, but not those occupying roles that are the traditional regulatory touchpoints. And even when operators can be identified, they may lack the ability to modify DeFi services or stop transactions because of the decentralized nature of the protocols. Smart contracts can interact with assets held by other smart contracts that are not directly associated with a particular user. Regulators will need to assess who is *responsible* and when a locus of responsibility must be identified. It may be possible to do so through careful analysis of services, even when they are nominally decentralized.[42]

Legal regimes often include mechanisms for vicarious secondary “controlling person”, “responsible officer” or aiding-and-abetting liability based on requirements such as knowledge or foresight of harmful consequences.[43] If developers of a DeFi service or others associated with the DeFi business *could have* identified and mitigated legal compliance risks, policy-makers will need to consider whether it is appropriate to mandate that they should have. On the other hand, regulating the creation of software raises important concerns of freedom of speech and administrability, which should be considered carefully. The borderless nature of blockchain networks and digital assets also poses challenges for DeFi regulation at the national or subnational level.

3.2 Available policy tools

There are many ways for a policy-maker to approach new financial services or products. Below, we first identify some helpful steps that regulators have taken in responding to the rise of digital assets and token offerings.

1. Transitional mechanisms

While not entirely analogous, policy approaches may be informed by how digital assets were initially addressed. In the 2017 initial coin offerings (ICOs) boom, few regulators had structures or expertise fit for purpose as – seemingly out of nowhere – significant capital was flowing into new platforms that claimed to be outside the regulatory perimeter. Some of the initial responses may prove useful in the context of DeFi.

Specialized regulatory units: A targeted desk with qualified staffing can serve as an initial gateway to gain experience in new technology, interact with the industry and provide guidance. This knowledge can be shared with policy-makers and actions may include issuing non-action letters under existing regulatory regimes. These groups may provide legal clarity to DeFi projects and encourage early-stage discussions with regulators. Regulators should also invest in technology and technical expertise to understand these markets more effectively. Many jurisdictions have used this approach. For example, the US Securities and Exchange Commission (SEC) created its FinHub unit (upgraded to a formal stand-alone office in late 2020), while Switzerland’s financial regulator, FINMA, created the FinTech Desk. Though initially small and limited in authority, they quickly became an important point of contact for both internal and external communities.

Incentivizing information flow: Disclosure is one of the most common tools of financial regulation. Even when the applicability of existing disclosure requirements on DeFi platforms is uncertain, efforts to encourage broad and consistent information disclosure may prove fruitful for regulatory analysis. The Monetary Authority of Singapore focused a significant portion of its regulation of ICOs on reviews of white papers.

Regulatory sandboxes: Policy-makers may decide to establish regulatory forbearance programmes such as sandboxes, where companies may test and operate their technology in a limited scope and therefore with limited regulatory risks. The scope of such regulatory “carve-outs” can be defined by activities, financial thresholds, territorial or customer limits and combined with reporting duties to ensure that the regulatory authority gains experience in new technology, interacts with the industry and reacts if new risks arise. However, a lack of transparency from the regulatory authority about the trajectory may inadvertently stifle innovation and there may be business risks involved for start-ups building in sandboxes without explicit safe harbours. The sandbox gives start-ups a chance to address regulatory compliance concerns and gives regulators a better understanding of the risks and benefits of a new space. A DeFi sandbox might go beyond the prior models by establishing a means of monitoring the trajectory for projects looking to decentralize control over time in order to address some concerns without creating new ones. The UK Financial Conduct Authority (FCA) established a sandbox regime for fintech that included a substantial number of blockchain and digital asset services. However, it has had limited applicability for DeFi because stablecoins are considered to be outside the FCA's scope. Others, such as Colombia´s "la Arenera" sandbox, have followed this approach as well. DeFi sandboxes will need to be designed carefully to avoid prematurely signalling approval from the regulator.

A variation of this approach is a *regulation-free zone*, as implemented in Busan, South Korea. Under this model, specific jurisdictions within a country may allow companies to operate under a limited set of regulations (often not fully "regulation-free") in order to allow for innovation and testing of services.

Clarifying easy cases. There will always be some new activities that clearly raise regulatory red flags, some that do not and others that are in grey areas. Sometimes by taking on the easier cases first, especially those where intervention is not warranted, policy-makers and regulators can narrow the zone of uncertainty and incentivize compliance activities. A more formal approach for distinguishing easy cases is a safe harbour policy that explicitly excludes from regulation services that meet defined criteria. In the ICO case, the US SEC's first official statement was the 2017 investigative report on the DAO.[44] It clarified that bitcoin was not considered a security, but that a token created for investment purposes would be. Further, because the DAO had already shut down, there was no need for an enforcement action. Though it left many questions unanswered, the report clarified the SEC's approach and its concerns, facilitating further dialogue.

Coordinating government action. In some cases, it may be useful to bring together different government entities for a harmonized response. An example is the modification of the "Volcker Rule" in the US by five federal regulatory agencies (the SEC, the Commodity Futures Trading Commission [CFTC], the Federal Deposit Insurance Corporation [FDIC], the Office of the Comptroller of the Currency [OCC] and the Federal Reserve Board).

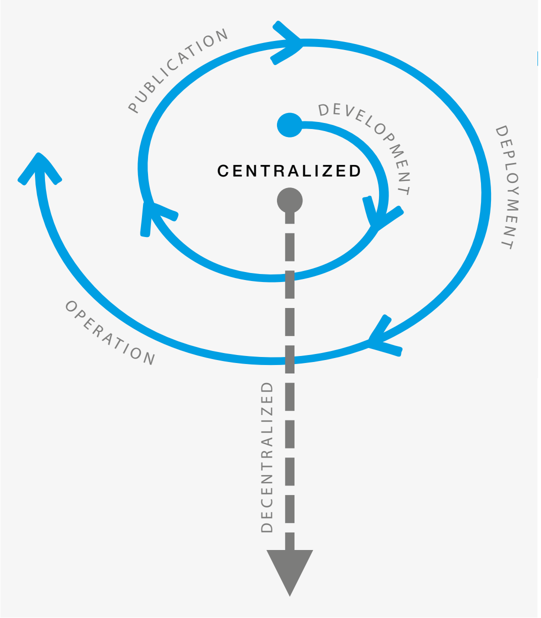
This list is not intended to be comprehensive. Nor does it presuppose the direction in which the policy-makers will eventually go. These techniques are equally relevant if DeFi services are ultimately found to be covered by existing requirements, outside the regulatory perimeter or subject to new, bespoke rules.

2. Regulation throughout the life cycle

Where there is no inherent distinctive risk, regulation typically occurs later in the life cycle of a product or service, when the harms that trigger liability or regulatory enforcement are more likely to occur. Early on, regulators are more likely to adopt a "do no harm" approach, given the relatively small scale and innovative potential of nascent technologies. For products with clearly known dangers or misuses, such as poppy flowers and weapons, the industry is strictly regulated and all stages are carefully supervised and controlled. Technological systems tend to fall somewhere in the middle.

In addition to maturing, DeFi services have the potential to become more decentralized across their life cycle, as detailed in **Appendix 3**. The degree of decentralization is also an important consideration for policy-makers and regulators. Rules to address the potential dangers of DeFi services can be adopted at four stages of the life cycle: (1) development; (2) publication; (3) deployment; and (4) operation, as shown in **Figure 4**.

FIGURE 4 | **DeFi service life cycle**



There will typically be an identifiable group of protocol developers (although it might operate under the umbrella of an open-source development community, non-profit foundation or association or the DAO). Once the protocol is published, multiple teams might develop it into services and market it to users, representing a combined deployment stage. Those services might later be forked by different teams. The operation of the service will largely be automated by the protocol and smart contracts, perhaps moderated by decentralized governance processes.

Imposing regulatory obligations may be easier earlier in the life cycle, where there may be clearly identifiable access points and more room to influence the long-term trajectory. However, the earlier in the life cycle, the weaker the nexus to actual demonstrable harm and the greater the potential implications for innovation – so it is important to determine at what point regulatory involvement is proportionate to the risks. Tools that incentivize rather than mandate action at early stages, including sandboxes, safe harbours and no-action letters, can be a valuable means of mediating this conflict.

3.3 Decision tree

This tool integrates frameworks presented in this toolkit to support internal policy and regulatory analysis of DeFi services. It is not intended to provide specific recommendations on when and how to act.

This may be used in conjunction with the other resources cited in this toolkit:

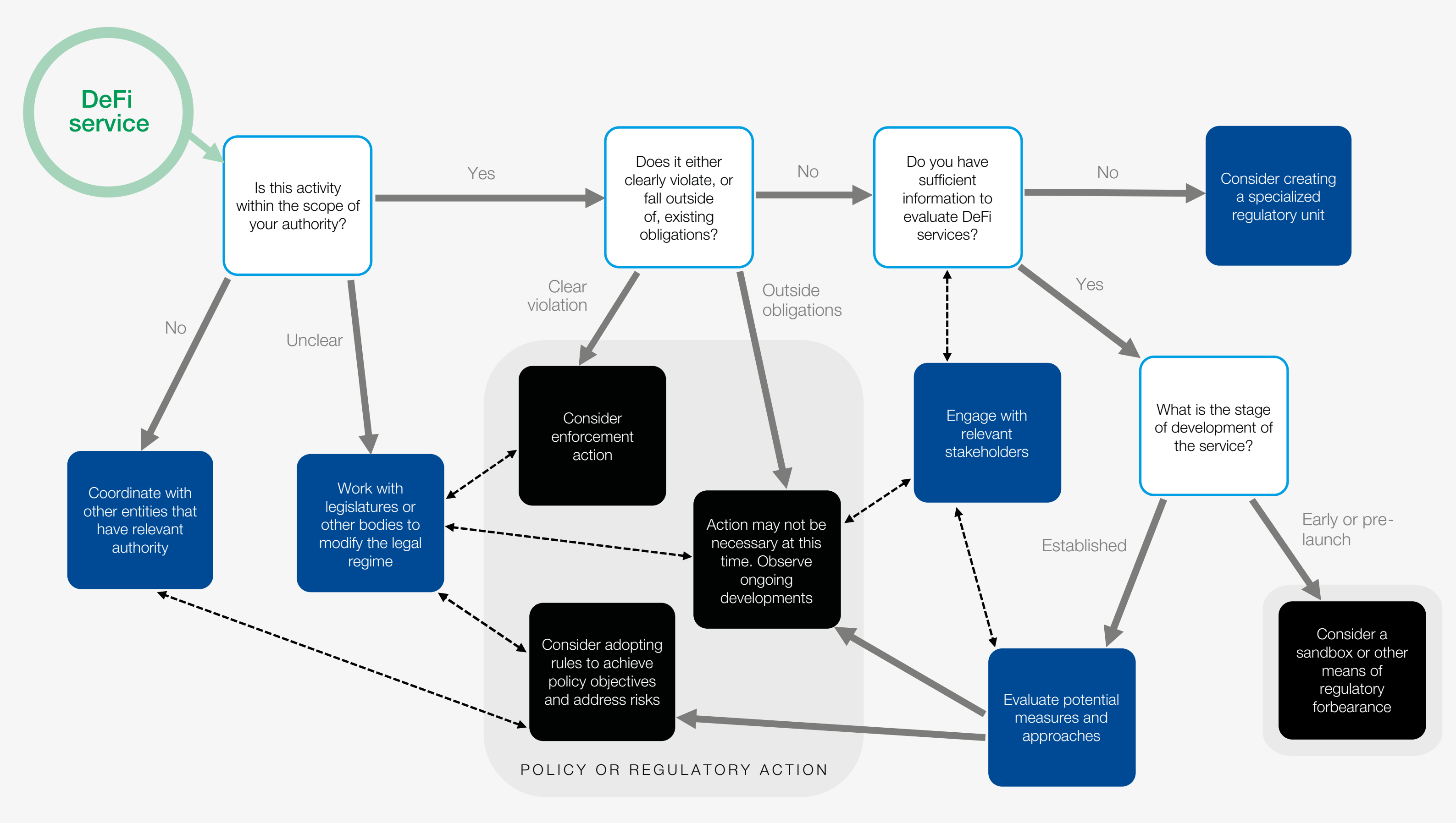
- **Appendix 1** offers a series of questions to identify relevant policy considerations and capabilities for DeFi generally.
- When considering a policy or protocol, the initial step, following **Figure 1**, is to determine whether the activity represents DeFi.
- **Figure 2** and the companion paper *DeFi Beyond the Hype* can be used to understand the relevant service categories and features.

If a service is considered DeFi:

- The questions shown below in **Figure 5** are designed to clarify the suggested courses of action.
- **Appendix 2** is a stakeholder mapping tool that can be used to identify relevant stakeholders for engagement.
- The decentralization spectrum in **Appendix 3** allows for a more precise picture of whether there are significant points of control in the service that might be relevant for decision-making.

Finally, when a determination to consider policy or regulatory action has been made, the policy-maker canvas in **Appendix 4** walks through a series of questions to assist in developing specific responses.

FIGURE 5 **Decision tree for evaluating DeFi services**


DeFi service
Is this activity within the scope of your authority?
Yes
Does it either clearly violate, or fall outside of, existing obligations?
No
Do you have sufficient information to evaluate DeFi services?
No
Consider creating a specialized regulatory unit
No
Unclear
Clear violation
Outside obligations
Yes
Coordinate with other entities that have relevant authority
Work with legislatures or other bodies to modify the legal regime
Consider enforcement action
Action may not be necessary at this time. Observe ongoing developments
Consider adopting rules to achieve policy objectives and address risks
Engage with relevant stakeholders
What is the stage of development of the service?
Established
Early or pre-launch
Evaluate potential measures and approaches
Consider a sandbox or other means of regulatory forbearance
POLICY OR REGULATORY ACTION

Conclusion

This toolkit is designed as a starting point for policy-makers seeking to understand the risks and opportunities posed by DeFi businesses and services, and to devise the best policy responses. The particular manifestations of DeFi, and the policy questions they pose, will change over time, as will activity levels and other aspects of the larger blockchain and digital asset world.

Policy-makers and regulators will take different approaches based on the unique context of their jurisdictions. Larger shifts in financial regulatory obligations, or implementation of cross-national standards, may alter the context for consideration of DeFi issues. There were no decentralized digital currency assets before 2009, and no general-purpose smart contract platforms before 2015, so any recommendations about the proper treatment of an offshoot such as DeFi must consider potential and unpredictable developments in a space that is evolving rapidly.

What is clear is that DeFi represents a distinct and potentially significant development, both within the landscape of blockchain and of financial services more generally. As this report has documented, DeFi presents a host of opportunities and many challenges. Even when there are no clear answers, policy-makers are best served by considering the right questions to ask, appreciating the points of interaction and tension with their regulatory regimes, and estimating the costs and benefits of various courses of action.

Appendix 1: Background assessment

The following questions are designed to help evaluate fundamental background questions before proceeding with policy or regulatory decisions.

Editable versions are available in Word and Excel form.

- Is DeFi, or a subset of DeFi services, within your entity's mandate? If so, what are the relevant policy or regulatory areas of focus? What are the top three risks you are focused on?

Top three risks:

1.

2.

3.

- Are there other entities that have relevant mandates? What are they? How do their jurisdictional scope and risk priorities compare to yours? What are your procedures, if any, for coordinating with those entities?

- Has DeFi been explored by your entity or others? What were the outcomes of those explorations?

- What is the in-house knowledge, experience and expertise related to DeFi? What about fundamentals such as digital assets, blockchain technology and decentralized governance?

- What is the process for getting up to speed on quickly evolving spaces and technologies? Are these relevant to DeFi or will they need to be adapted?

- Which parties in the public or private sector are required to provide input or consultation regarding potential changes in policies/regulations related to the financial system and financial technology?

- From which institutions or parties would it be beneficial to solicit input? Which additional stakeholders should be represented and involved in decision-making?

Appendix 2: Stakeholder mapping tool

This tool is designed to help policy-makers map out the relevant environment of a given DeFi service. We group stakeholders into four categories, though in some cases stakeholders may span multiple categories:

- **Builders**: create, implement and support DeFi protocol
- **Suppliers**: provide capital or a core service to the functioning of the protocol
- **Users**: use protocol functionality for intended use case
- **Governance**: make decisions on the development of the protocol

1. For each service, use the stakeholder mapping table to identify who or what the relevant actors are for each category. The more specific, the better. Every category may not be represented, or there may be multiple entries in a category.
2. Review relevant materials, such as white papers, source code, etc. to identify:
    a. The specific obligations on each actor
    b. The specific rewards each actor hopes to receive (in the form of fees, value accrual, categories or other metrics as specified by the protocol).

Complete one stakeholder map per DeFi protocol or service. Blank rows are spaces to add additional stakeholders, where relevant.

Editable versions are available in Word and Excel form.

Protocol or service name:

Service category (See Part IC)

Category	Stakeholders	Responsibility/impact	Economic incentives	Obligations	Rewards
Builders	Interface providers	Provide access to DeFi protocols, either directly or through aggregation	Receive transaction fees		
	Auxiliary service providers	Support external data feeds, or offer development tools for DeFi services	Receive transaction fees		
	Connected protocols	Other composable protocols integrated with the target service	Drive utility for their protocol, generate fees		
	Wallet providers	Protect user funds	Fees based on assets		
Builders and governance	Development teams	Drive development of a protocol and ecosystem	Receive inflationary rewards and transaction fees		
Governance	Multisig signatories	Shape governance to ensure long-term sustainability	Earn proportion of fees generated by the protocol		
	Governance token holders	Propose and vote on governance decisions	Earn proportion of fees generated by the protocol		
	Miners or stakers	Verify transactions on the underlying blockchain	Receive inflationary rewards and transaction fees		
Suppliers	Liquidity providers	Contribute collateral or other assets to facilitate DeFi activity	Receive inflationary rewards and transaction fees		
	Liquidators	Liquidate under-collateralized positions	Obtain collateral at discount		
Users	Protocol users	Use protocol functionality for intended use case	Low-cost, peer-to-peer, trust-minimized financial services		
	Protocol token holders	Use protocol functionality or purchase tokens on secondary markets	Profit from appreciation of token value, or receive inflationary rewards and transaction fees		

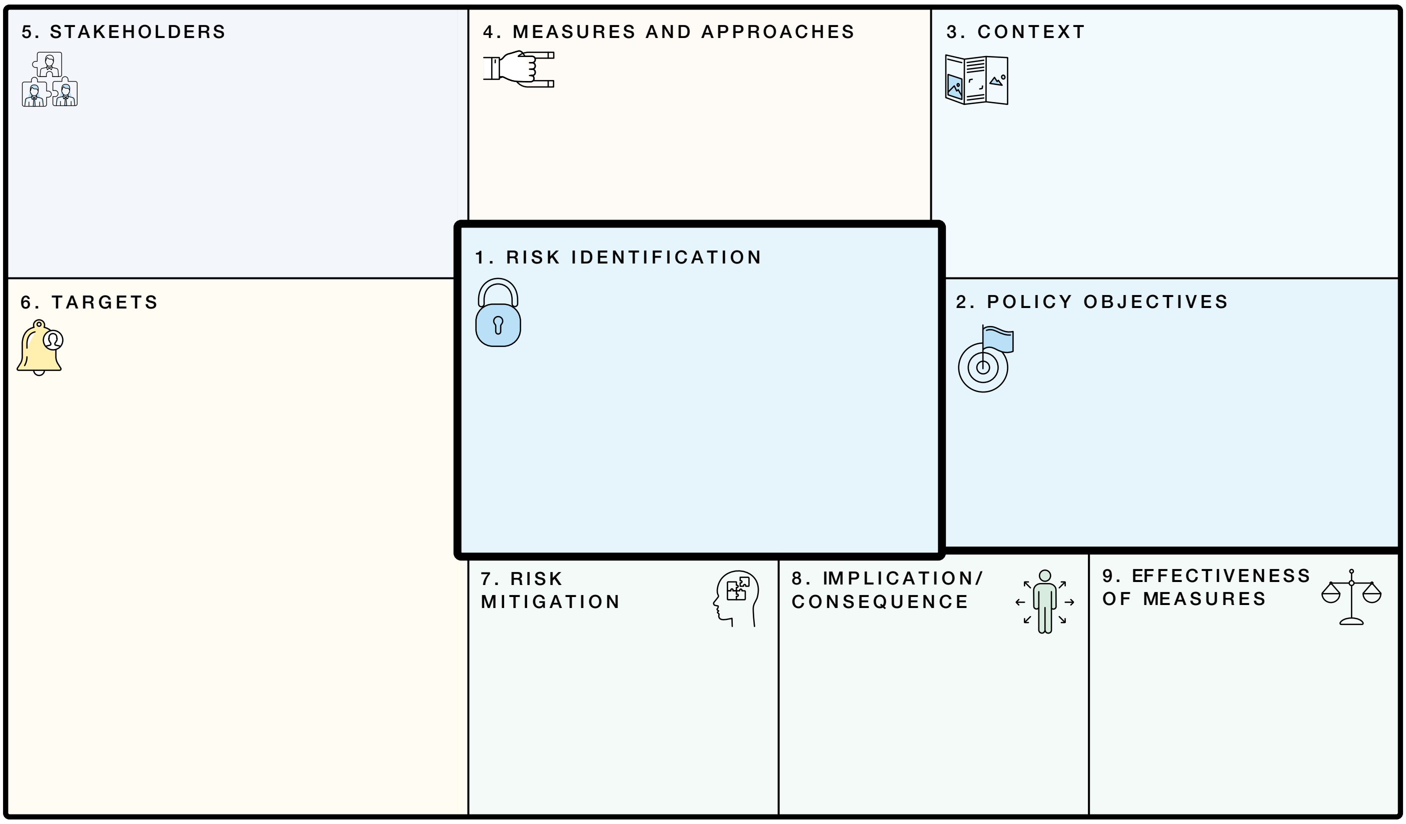
Appendix 3: Decentralization spectrum

Several aspects of DeFi protocols or services may be more or less decentralized. Furthermore, decentralization can occur at the asset level, at the smart contract level and at the protocol level, to varying degrees.[45] The following tool maps out the relevant questions to evaluate the spectrum of decentralization in each major area.

Key questions		Potential spectrum		
Governance	Who decides which aspects of the system can be altered by governance token holders? What is the threshold to propose governance change? What percentage of token holders needs to vote on proposal for vote to be valid? Who can vote (all users, all token holders, only governance token holders)? Are all governance tokens freely traded?	**Completely centralized** Only operators can change any aspects of the system	**Partially decentralized** Only some aspects can be altered by governance token holders; threshold for proposing governance change is low	**Completely decentralized** All aspects can be altered, any token holder can propose change
Custody	Who is in charge of safely guarding the assets? Does the user retain control over funds at all times? Who controls the multisignature wallet of the protocol? Are admin keys controlled by a DAO? Are admin keys held in cold storage?	**Fully custodial** Service retains full control of assets	**Partially non-custodial** Admin key, time-lock and/or multisig for updating parameters	**Completely non-custodial** Customer has full control of assets
Protocol modification	Once a smart contract is deployed, can the code be changed by a party unilaterally? Which parties can make changes to the protocol?	**Completely centralized** Operators alone can modify all parameters	**Partially decentralized** Operators can change some parameters; users can change other parameters	**Completely decentralized** User alone can modify all parameters
Verifiable security	Does the development team offer a public bug bounty programme? Has there been at least one audit of the code deployed on-chain? Has the audit report been made public? Have all of the serious issues listed in the report been fixed? Have any vulnerabilities been exploited?	**No verifiable security** Not transparent and unaudited	**Some verifiable security** Either transparent or audited	**Fully verifiable security** Formal public verification, with audits from top security firms and a bug bounty programme
Insurance coverage	Is there insurance coverage? For which risks? Up to what amount? Is the insurer able to withstand a "black swan event" in DeFi (e.g., substantial coverage claims from different DeFi users simultaneously)?	**No coverage** Assets are uninsured	**Some coverage** Limited or non-standardized coverage	**Full coverage** Assets fully insured

Appendix 4:
DeFi policy-maker canvas

The following tool has been developed to help policy-makers frame their consideration of potential approaches to DeFi businesses.[46] It is designed to apply key components of this toolkit in a structured manner. **Editable versions are available in Word and Excel form.**



5. STAKEHOLDERS

4. MEASURES AND APPROACHES

3. CONTEXT

1. RISK IDENTIFICATION

6. TARGETS

2. POLICY OBJECTIVES

7. RISK MITIGATION

8. IMPLICATION/ CONSEQUENCE

9. EFFECTIVENESS OF MEASURES

The canvas is intended to be used working out from the middle counterclockwise, and puts risk identification at its core. The canvas consists of nine questions divided into three stages:

(1) Identifying the necessity and conditions for policy-making

1. *What specific risk are you aiming to address?*

2. *What policy objectives will be achieved by addressing such risk?*

3. *What is the context in which the policy measure will be implemented?*

(2) Defining the approach

4. *What policy measures or approaches are you considering?*

5. *Who are the stakeholders likely to be affected by these measures or approaches?*

6. *Who would be required to take action to implement the measures or approaches?*

(3) Refining the approach

7. *Is there already risk mitigation in place (either tech-based or of a self-regulatory nature) and is it sufficient?*

8. *What would be the implication of this measure, especially regarding innovation, the core business model and Sustainable Development Goals (SDGs)?*

9. *How effective are these measures, i.e. regarding enforcement?*

1. Risk identification

The canvas puts the identified risks at the centre of the policy-making process. As outlined, DeFi may introduce a risk profile different from that presented by conventional financial activities.

As a basis for assessing harms, risks and responses in a structured way, the following questions may be relevant:

– What is the risk and who might suffer harm?
– How significant is the risk to a desired policy outcome?
– Who has a role in reducing/mitigating the risk? What can be done by that entity to mitigate potential harm?
– What legal mechanisms can address that harm?
– How might cross-border activity be addressed?

Example: Operational risks regarding custody (loss of funds)

2. Policy objectives

Before developing a specific approach, policy-makers should identify priorities for policy outcomes. These should serve as a basis for weighing the implications based on proportionality at a later stage (see Refining the approach, above).

Example: Investor protection and financial stability

3. Context

It will be important to understand where DeFi policies and regulations fit within broader regulatory schemes. There may also be existing market structure issues or areas of particular concern in the relevant jurisdiction that bear on decisions concerning DeFi.

Example: National initiatives to promote local development of innovative financial service platforms

4. Measures and approaches

Depending on the layer of the “DeFi stack” addressed, legal mechanisms to address the identified risk of harm will vary. Approaches should be crafted accordingly.

Example: [Gateway] – licensing regime for custodians

5. Stakeholders

This step identifies the groups or categories of individuals who might be affected, positively and negatively, by the proposed measures or approaches.

Example: Investors seeking to leverage their digital assets to increase potential returns; liquidity providers seeking predictable yields for digital assets they hold

6. Targets

This step analyses which actors need to implement the policy or would be encumbered by the measures involved. Activities could be grouped to identify roles, which would then inform specific obligations and controls.

Example: Someone who has control over private keys for others (custodian)

7. Risk mitigation

Policies and regulations should take into consideration existing risk mitigation, which may be tech-based or self-regulatory. It is likely that these will require supplementary measures, but this will give a more informed and nuanced picture of risk.

Example: Self-custody with multisignature wallet and smart contract-enabled governance features (threshold, white-listed addresses, etc.) and auditing of smart contracts

8. Implication/consequence

Desired policy outcomes will need to balance investor protection, innovation and many other considerations. Some measures and approaches will impose significant limitations on DeFi business models. Different levels of impact could be distinguished, for example:

- A low impact if the activity can be conducted without prior approval
- A medium impact if the operation cannot be performed without prior approval
- A high impact if such approval cannot be obtained at all due to the underlying decentralized business model

Example: Licensing regime for custodians = medium impact

9. Effectiveness of measures

As with all policies, the effectiveness of a measure – whether the measure can be enforced and how well it achieves the objective pursued – is an important consideration. Policy-makers and regulators should be clear about how they intend to measure the impact of the policy, weighing both the upsides and downsides, as defined by policy goals and objectives. Key metrics could explore the balance of areas such as consumer protection, privacy, innovation, etc. This also depends heavily on which layer of the tech stack a measure addresses. For instance, policies addressing the network infrastructure layer (blockchain protocol layer) will have more significant and far-reaching implications, and the effects should be measured and considered accordingly.

Example: High effectiveness where regulatory access point can be identified

Contributors

The World Economic Forum's Centre for the Fourth Industrial Revolution's work is global, multi-industry and multistakeholder. The project engages stakeholders in various industries and governments from around the world. This report is based on discussions, workshops and research, and the combined effort of all involved. Opinions expressed herein may not necessarily correspond with those of each person involved in the project, nor does it necessarily represent the views of their organizations.

Lead Authors

Sumedha Deshmukh
Platform Curator – Blockchain and Digital Assets, World Economic Forum, USA

André Geest
Researcher, Ludwig Maximilian University, Germany

David Gogel
Growth Lead, dYdX, USA

Daniel Resas
Associated Partner, Schnittker Möllmann Partners, Germany

Christian Sillaber
Senior Researcher, University of Bern, Switzerland

Editor

Kevin Werbach
Professor of Legal Studies and Business Ethics and Director, Blockchain and Digital Asset Project, Wharton School, University of Pennsylvania, USA

The authors would like to thank the following groups and individuals for their insights and contributions:

Content Contributors

Nic Carter, Partner, Castle Island Ventures, USA
Jake Chervinsky, General Counsel, Compound, USA
Tarun Chitra, Chief Executive Officer, Gauntlet, USA
Ann Sofie Cloots, Slaughter & May Lecturer in Company Law, University of Cambridge, United Kingdom
Jacek Czarnecki, Global Legal Counsel, Maker Foundation, Poland
Brendan Forster, Chief Operating Officer, Dharma Labs, USA
Katharina Gehra, Chief Executive Officer, Immutable Insight, Germany
Andreas Glarner, Partner, MME Legal Tax Compliance, Switzerland
Jordan Lazaro Gustave, Chief Operating Officer, Aave, United Kingdom
Siân Jones, Senior Partner, XReg Consulting, Gibraltar
Daniel Kochis, Global Head of Business Development, Chainlink Labs, USA
Joyce Lai, Member, New York Angels; Founder, NewTerritories.io, USA
Urszula McCormack, Partner, King & Wood Mallesons, Hong Kong SAR
Fabian Schär, Professor for Distributed Ledger Technology/Fintech, University of Basel, Switzerland
Lex Sokolin, Head Economist and Global Fintech Co-Head, ConsenSys, United Kingdom
Teana Baker Taylor, General Manager, UK, Crypto.com, United Kingdom

Acknowledgements

Content Reviewers

Marcos Allende Lopez, Technical Leader, LACChain, Inter-American Development Bank, USA
Marvin Ammori, Chief Legal Officer, Uniswap Labs, USA
Sebastian Banescu, Senior Research Engineer, Quantstamp, Germany
Matthias Bauer-Langgartner, Technical Specialist, FCA Innovate, United Kingdom
Nicolas Brügger, Senior Policy Adviser, State Secretariat for International Finance, Switzerland
Jehudi Castro Sierra, Digital Transformation Adviser, Office of the Presidency, Colombia
Charles Dalton, Software Engineer, Blockchain, Crypto, and Digital Currencies, PayPal, USA
Maxim Galash, Chief Executive Officer, Coinchange, Canada
Oli Harris, Vice-President, Goldman Sachs, USA
Kibae Kim, Principal Researcher, Korea Policy Centre for the Fourth Industrial Revolution, KAIST, South Korea
Netta Korin, Co-Founder, Orbs; Founder, Hexa Foundation, Israel
Ashley Lannquist, Project Lead, Blockchain and Digital Currency, World Economic Forum, USA
Caroline Malcolm, Head, Global Blockchain Policy Centre, Organisation for Economic Co-operation and Development, France
Rob Massey, Tax Blockchain, Crypto and Digital Assets Leader, Deloitte, USA
Paul Maley, Global Head of Securities Services, Deutsche Bank, United Kingdom
Xavier Meegan, Blockchain Intern, ING, Netherlands
Michael Mosier, Acting Director, FinCEN, USA
Michael Oh, Director, Office of Financial Innovation, FINRA, USA
Sam Proctor, Chief Executive Officer, Genesis Block, USA
Lane Rettig, Core Team, Spacemesh, USA
Richard Rosenthal, Risk and Financial Advisory, Banking Regulatory Specialist, Deloitte, USA
Lukas Staub, Senior Legal Adviser, State Secretariat for International Finance, Switzerland
Christoph Simmchen, Legal Counsel, Gnosis, Germany
Sheila Warren, Deputy Head, Centre for the Fourth Industrial Revolution, World Economic Forum, USA

Many thanks also to the policy-makers, regulators and industry leaders, both listed and unlisted, who shared their valuable time and insights in roundtables, in individual conversations, and through written feedback.

Editing and Design

Bianca Gay-Fulconis, Designer
Elizabeth Mills, Acting Head of Editing
Alison Moore, Editor

Endnotes

1. We use the general term “digital asset” rather than “cryptocurrency”, “virtual currency” or “cryptoasset”. Particular terms may have distinct legal meanings in certain jurisdictions.
2. The Defiant, “Exclusive: DeFi Year in Review by DappRadar”, 28 December 2020: https://thedefiant.substack.com/p/exclusive-defi-year-in-review-by-1f2 (link as of 12/5/21).
3. While Bitcoin technically operates on the basis of limited-function smart contracts, Ethereum is a Turing complete blockchain, meaning that it can theoretically support any application that can be executed on a computer.
4. The Defiant, “Exclusive: DeFi Year in Review by DappRadar”, 2020.
5. ConsenSys, *The Q1 2021 DeFi Report*, May 2021: https://consensys.net/reports/defi-report-q1-2021/ (link as of 12/5/21).
6. Jesse Walden, “How Does DeFi Cross the Chasm?”, 17 June 2020: https://jessewalden.com/how-does-defi-cross-the-chasm/ (link as of 12/5/21).
7. Linda Xie, “A Beginner’s Guide to DeFi”, 3 January 2020: https://nakamoto.com/beginners-guide-to-defi/ (link as of 12/5/21).
8. https://rekt.news/leaderboard/ tracks incidents. One research firm identified nearly $300 million lost in DeFi hacks between July 2019 and February 2021: https://cointelegraph.com/news/defi-hacks-and-exploits-total-285m-since-2019-messari-reports; Chainalysis estimated that $34 million of DeFi transactions were conducted by criminal actors: https://coinmarketcap.com/headlines/news/34-million-in-defi-crime-2020/ (links as of 12/5/21).
9. Miles Kruppa and Hannah Murphy, “‘DeFi’ Movement Promises High Interest but High Risk”, Financial Times, 30 December 2019: www.ft.com/content/16db565a-25a1-11ea-9305-4234e74b0ef3 (link as of 12/5/21).
10. Fabian Schär, “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets”, 2020: https://ssrn.com/abstract=3571335; Dirk Zetzsche et al., “Decentralized Finance”, Journal of Financial Regulation 6(2), pp. 172–203, 2020: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194 (links as of 12/5/21).
11. DeFi market participants often describe services as “protocols” because they are the software code embodied in smart contracts running on the blockchain network. Formally, however, protocols are the technical specification that the software implements.
12. Projects might start out using a centralized implementation with a defined path towards a trust-minimized ecosystem.
13. Products and services offered through permissioned networks and/or blockchains provide additional layers of control and centralization with a distinct risk profile not covered in this report.
14. While Bitcoin is generally not a DeFi foundation because it offers limited smart contract functionality, bitcoin is widely used as a form of collateral for DeFi services, providing bitcoin holders with new options for returns on their holdings.
15. “Custodial” here refers to control over assets, not software code. There may or may not be an entity that has the ability to make unilateral changes to the DeFi protocols or services. Further, we use the term in the colloquial sense of having the ability to move or manipulate assets without the involvement of their owner, not based on any legal definition of “custody” in financial regulation. There are established legal and regulatory requirements governing how customer assets are controlled, such as SEC Rule 15c3-3, which differ from jurisdiction to jurisdiction.
16. European Central Bank, “ESCB/European Banking Supervision Response to the European Commission’s Public Consultation on a New Digital Finance Strategy for Europe/FinTech Action Plan”, 2020:
17. To date, DeFi ecosystems primarily operate on a single blockchain platform. Cross-chain interoperability is the subject of a number of different initiatives.
18. For a similar representation and further analysis, see Schär, “Decentralized Finance”.
19. Sebastian Sinclair, “Uniswap’s First Governance Vote Ends in Ironic Failure”, Coindesk, 20 October 2020: https://www.coindesk.com/uniswaps-first-governance-vote-ends-in-ironic-failure (link as of 12/5/21).
20. Some algorithmic stablecoins attempt to maintain sufficient collateralization dynamically as prices shift; others dynamically adjust supply.
21. We use the term “credit” to cover borrowing and lending relationships broadly, rather than in the technical sense of money creation. In contrast to arrangements such as bank loans, in which the borrowing process is separate from the pooling of capital to fund those loans, DeFi services can provide both sides simultaneously, often targeting the same users.
22. Hugh Karp, “Comparing Insurance-Like Solutions in DeFi”, DeFi Prime, 19 November 2019: https://defiprime.com/comparing-insurance-like-solutions-in-defi (link as of 12/5/21).
23. It bears noting that many blockchains used for DeFi employ proof-of-stake consensus, which does not involve computationally intensive mining. Ethereum, the blockchain supporting the most DeFi activity, plans to transition to proof-of-stake, as well. Ethereum Foundation, *The Eth2 Upgrades: Upgrading Ethereum to Radical New Heights*: https://ethereum.org/en/eth2/ (link as of 12/5/21).
24. See case study in Section 2.2.

[25] E. J. Spode, “The Great Cryptocurrency Heist”, Aeon, 14 February 2017: https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum (link as of 12/5/21).

[26] William Foxley, “Everything You Ever Wanted to Know About the DeFi ‘Flash Loan’ Attack”, Coindesk 19 February 2020: https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack; Yogita Khatri, “Balancer Pools Drained of More Than $450,000 Due to an Exploit Connected to Deflationary Tokens”, The Block, 29 June 2020: https://www.theblockcrypto.com/linked/69785/balancer-pools-drained-of-more-than-450000-due-to-an-exploit-connected-to-deflationary-tokens; William Foxley, “Origin Protocol Loses $7M in Latest DeFi Attack”, Coindesk, 17 November 2020: https://www.coindesk.com/origin-protocol-loses-3-25m-in-latest-flash-loan-attack-reports (links as of 12/5/21).

[27] Connor Sephton, “Overall Losses from Crypto Hacks Are Down – but DeFi Attacks Have Surged”, Modern Consensus, 10 November 2020: https://modernconsensus.com/cryptocurrencies/overall-losses-from-crypto-hacks-are-down-but-defi-attacks-have-surged/ (link as of 12/5/21).

[28] Ethereum Foundation, *The Eth2 Upgrades*.

[29] C. Sillaber and B. Waltl, “Life Cycle of Smart Contracts in Blockchain Ecosystems”. DuD 41, 497–500 (2017). https://doi.org/10.1007/s11623-017-0819-7 (link as of 28/5/21).

[30] Klint Finley, “A $50 Million Hack Just Showed That the DAO Was All Too Human”, Wired, 18 June 2016: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ (link as of 12/5/21).

[31] Flashbots, created by researchers in this area, publishes open-source software that miners use for transparent allocation of MEV. However, the approach is controversial; Alex Obadia, “Flashbots: Frontrunning the MEV Crisis”, 23 November 2020: https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752 (link as of 28/5/21).

[32] Philip Daian et al., “Flash Boys 2.0: Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges”, IEEE Symposium on Security and Privacy, 2020: https://arxiv.org/abs/1904.05234 (link as of 12/5/21).

[33] Scott Chipolina, “Oracle Exploit Sees $89 Million Liquidated on Compound”, Decrypt, 26 November 2020: https://decrypt.co/49657/oracle-exploit-sees-100-million-liquidated-on-compound (link as of 12/5/21).

[34] Forks of a decentralized application codebase are distinct from forks of the blockchain settlement layer, such as the split of Ethereum and Ethereum Classic. The forks described here are more analogous to those of other open-source software projects, which create a competing alternative rather than splitting the transaction history.

[35] The Defiant, “SushiSwap’s Vampire Scheme: Hours Away and with $1.3B at Stake”, 8 September 2020: https://thedefiant.substack.com/p/sushiswaps-vampire-scheme-hours-away (link as of 12/5/21).

[36] Matthias Nadler and Fabian Schär, “Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution”, IEEE Symposium on Security and Privacy, 2020: https://arxiv.org/abs/2012.09306 (link as of 12/5/21).

[37] Ian Allison, “Inside the Standards Race for Implementing FATF’s Travel Rule”, Coindesk, 4 February 2020: https://www.coindesk.com/inside-the-standards-race-for-implementing-fatfs-travel-rule. FATF draft guidance published in March 2021 suggested that DeFi developers and services might face additional compliance obligations. Nikhilesh De, “State of Crypto: FATF’s New Guidance Takes Aim at DeFi”, Coindesk, 30 March 2021: https://www.coindesk.com/fatfs-new-guidance (links as of 12/5/21).

[38] As an early example of such integration, MakerDAO has incorporated a pool of real estate assets into the collateral base for its stablecoin. Muyao Shen, “Maker Price Passes $4K for First Time, as MakerDAO Brings Real Estate to DeFi”, Coindesk, 21 April 2021: https://www.coindesk.com/maker-price-makerdao-real-world-assets-defi (link as of 12/5/21).

[39] Brady Dale, “Mempool Manipulation Enabled Theft of $8M in MakerDAO Collateral on Black Thursday: Report”, Coindesk, 22 July 2020: https://www.coindesk.com/mempool-manipulation-enabled-theft-of-8m-in-makerdao-collateral-on-black-thursday-report (link as of 12/5/21).

[40] Appolline Blandin et al., “Global Cryptoasset Regulatory Landscape Study”, Cambridge Centre for Alternative Finance (2019), p. 41: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf (link as of 12/5/21).

[41] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets”, 2019/1937: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 (link as of 12/5/21).

[42] US Securities and Exchange Commission, “SEC Charges EtherDelta Founder with Operating an Unregistered Exchange”, news release, 18 November 2018: https://www.sec.gov/news/press-release/2018-258 (link as of 12/5/21).

[43] US Commodity Futures Trading Commission, “Remarks of Commissioner Brian D. Quintenz at the 38th Annual GITEX Technology Week Conference”, 16 October 2018: https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16; Aaron Wright and Gary DeWaal, “The Growth and Regulatory Challenges of Decentralized Finance”, presentation to the US Commodity Futures Trading Commission Technology Advisory Committee Virtual Currency Subcommittee, 14 December 2020: https://www.youtube.com/watch?v=-gDFXiudwl4&feature=youtu.be (links as of 12/5/21).

[44] US Securities and Exchange Commission, “Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO”, release no. 81207, 25 July 2017: https://www.sec.gov/litigation/investreport/34-81207.pdf (link as of 12/5/21).

[45] Modified from Tony Sheng and Ben Sparango, “Trust Spectrum”: https://multicoin.capital/2020/03/24/trust-spectrum/ (link as of 12/5/21).

[46] The DeFi Policy-Maker Canvas is built upon the Digital Policy Model Canvas created by the Transnational Network on National Digital Policy at the World Economic Forum, 15 September 2017.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org