Primer on DeFi: Risks and Regulations

The Ecosystem Is Not Yet Systemic, but Many Risks Lurk and Regulation Beckons

Key Characteristics of the DeFi Ecosystem

Key DeFi Services	DeFi Disruptive Elements
Savings and investments	Fully public, no intermediaries
Asset trading/exchange	Users control their assets
Digital asset loans	Automated, composable
Insurance services	Multiple (atomic) transactions
Asset management	Non-stop market hours

Source: Fitch Ratings

This report is part of a companion series with Primer on DeFi: The Ecosystem examining the characteristics of the DeFi ecosystem, the key DeFi services and the blockchain networks that underpin the infrastructure and settlement of DeFi.

Accelerates the 'Finance as a Service' Model

Decentralised finance (DeFi) accelerates the existing trend of providing "finance as a service", bypassing mainstream centralised financial (CeFi) intermediaries to offer an alternative to existing banks, fintechs, and other financial institutions. Its user base appears to be concentrated within India, China, the US, Vietnam, Thailand, Brazil, the UK and Russia.

The inherent flexibility, interoperability, and openness of DeFi applications (dapps), allied to a lack of regulatory oversight, facilitates product innovation. Users can execute complex multi-legged and leveraged transactions which settle simultaneously. The technology underpinning DeFi can theoretically help with other technology to reduce CeFi's operational, credit and settlement risks – but carry risks of their own, some unique to DeFi.

Risks to Wider Financial System Are Limited

DeFi presents limited risks to the mainstream financial system as, barring stablecoins, it is largely separate and not yet systemic in size. The total value locked in DeFi was around USD180 billion as of January 2022, up from USD22 billion at the start of 2021, although month-on-month growth is slowing. Banks' and insurance companies' links to DeFi are not yet material, and crypto-related funds invested about USD50 billion into DeFi in 2021.

Alongside market and liquidity risks, fraud is a significant risk with DeFi transactions. "Rug pull" scams, where developers abandon projects and take users funds, are prevalent, alongside phishing and code bugs. The manipulation of token prices is another threat. The immaturity of the sector is likely to lead to further exploits and risks.

Regulatory Views Will Likely Bifurcate DeFi

While Chinese and potentially Russian authorities effectively ban citizens' participation within DeFi and private digital assets, other authorities appear more likely to regulate elements of DeFi. This is likely to divide the sector, leading to a regulated strand gaining market acceptance and an innovative but unregulated segment.

Rating Views Evolving, but Red Lines Exist

Fitch Ratings' view on this sector will evolve as our understanding of risks improves, guided by regulatory and legal considerations. However, certain elements are unrateable, namely illegal activities or those subject to licensing or other prohibitions, structural elements outside standard market practice and Fitch's rating criteria, or the lack of a clear centre of economic interest within a jurisdiction.

Related Research

Cryptocurrency and Digital Assets Research

Primer on DeFi: The Ecosystem (February 2022)

Stablecoins: Regulatory Approaches and Credit Considerations (December 2021)

Crypto Rating Considerations and Use Case Assessments (Corporates and Financial Institutions) (October 2021)

Cryptocurrencies and Digital Assets: Cautious Entry for U.S. Banks (September 2021)

Analysts

Monsur Hussain
+44 20 3530 1793
monsur.hussain@fitchratings.com

What Is Decentralised Finance

Although there is no consensus on a definition of DeFi, it is generally characterised as a global ecosystem of web applications and electronic wallets that leverage computer programs or smart contracts stored on public blockchains, without requiring a centralised trusted intermediary, such as bank, or a traditional exchange (see *Annex* for key terms).

DeFi's key characteristics include the following features (see the companion report *A Primer on DeFi: The Ecosystem*):

- **Public, Open:** Dapps and protocols are public, with any user being able to access DeFi as long as they have an internet connection and a compatible electronic wallet;
- **Direct, Automated:** DeFi users transact on an automated direct peer-to-peer basis, relying on pre-defined rules, governed by a consensus mechanism to verify, agree and settle transactions;
- **Non-Custodial:** Users retaining control over their assets, which cannot be moved by third parties;
- **Lego-Like Composability:** DeFi protocols are coded using open software standards, with theoretically no limitation on what types of protocols can be interconnected, or how asset balances encumbered are used;
- **Crypto-Based:** The DeFi ecosystem uses digital assets such as stablecoins and floating value crypto tokens, rather than fiat currencies;
- **Transparent:** Digital records from DeFi transactions are public and transparent. Settlement is recorded on public permission-less blockchains that are visible to all parties; and
- **Lack of KYC, AML Checks:** DeFi does not generally require "know-your-customer" (KYC) identification reviews or anti-money-laundering (AML) checks: which can aid financial inclusion in jurisdictions with higher portions of under or unbanked populations, at the risk of making DeFi attractive to criminals.

In principle, any existing financial service can be represented within the DeFi ecosystem, provided it can be built with software. However, most dapps have focused on trading, lending and investing services that are linked to general speculation in digital assets, such as cryptocurrencies.

Disruptive Model Is Not Yet Affecting Other Financial Institutions

Bypassing mainstream financial institutions marks DeFi as a disruptive operating model. However, its current limited scale (see below) means that is it not yet disrupting the business models of mainstream financial institutions.

Existing financial institutions are piloting the use of technologies that underpin aspects of DeFi, e.g. the use of blockchains, albeit operating as private high-trust networks. To this end, it is not inconceivable for mainstream financial institutions to consider employing DeFi-like software protocols within a private blockchain network, as a suite of applications or financial tools. However, this arrangement is unlikely to be characterised as "DeFi".

DeFi Use Appears to Be Geographically Concentrated

Based on analysis of estimated values of digital assets received on blockchain networks and weighting the values based on purchasing power parity per capita, the adoption of DeFi appears to be strongest within India, China, the US, Vietnam, Thailand, Brazil, the UK and Russia (source: Chainalysis 2021 Geography of Cryptocurrency). Whereas smaller transaction volumes appear to be driven mainly by emerging market economies, the larger transaction volumes measured in millions of US dollars appear to be driven by users in the US, China, Russia and western Europe.

Rating Considerations

Fitch views digital assets and emergent ecosystems linked to them, such as DeFi, the broader tokenisation of assets, and the metaverse, as both risks and potential growth opportunities for financial institutions and corporates. While the effects to our rated universe are minimal to date, the digital asset ecosystem is still very young and may evolve in an unpredictable manner. We believe issuers could increase their direct or indirect exposure to cryptos and DeFi, should consumer or institutional adoption continue to grow, and not be derailed by new regulations.

From a rating perspective, Fitch's views will be guided by regulatory and legal considerations, and market developments. Considerations for current and prospective rated issuers' exposure to DeFi and crypto assets include:

- if there is a clear economic centre of interest within a jurisdiction (or across defined jurisdictions) with requisite oversight or appropriate licensing (to gauge the degree of regulatory uncertainty);
- whether the construct can be rated under criteria;
- market and liquidity risks (especially price volatility);
- counterparty risks, or risks linked to the execution of liquidation processes;
- operational and legal certainty;
- cybersecurity and software risks;
- consumer protection;
- revenue/EBITDA growth;
- disruptive business models;
- extent of crypto balance-sheet exposure; and
- gauging the potential use for illicit activities or tax evasion.

Fitch also sees several positive rating drivers for digital asset-sensitive issuers, most notably, incremental products/services and strong revenue and cash flow growth that could be supportive of financial profiles, provided market positions prove durable and defensible. However, Fitch believes crypto-focused institutions are more prone to tail risk events, which could lead to a meaningful erosion of firms' credit profiles, compared with traditional financial institutions.

Crypto or digital-focused financial institutions can be rated by Fitch but they are likely to be limited to below investment-grade levels. This is until further evolution and maturation of operating, legal and regulatory frameworks governing digital assets leads to a clearer legal status of crypto instruments and improved investor protections.

Perhaps more pressing from a rating perspective is the potential disruptive effect that cryptos and blockchain/DeFi technologies could have on traditional financial institutions and legacy payment networks. Fitch will consider the pace of crypto/blockchain adoption and corresponding reactions of traditional financial institutions when assessing potential negative implications to business models and profitability. The pace and magnitude of such structural shifts will be considered in deciding whether negative rating actions are warranted, although potential crypto-driven rating implications would likely only be realised over a long-term time horizon.

What Risks Are There Now for FIs?

DeFi and Crypto Risks Are Not Yet Material for CeFi

Aside from interconnections via stablecoins (see below), DeFi by its construction and reliance on digital assets is largely self-contained within its own ecosystem, and significant price corrections within the USD1.7 trillion crypto market (at end-January 2022) have not affected the mainstream financial sector, which suggests that financial stability risks are limited.

However, as this area continues to develop and expand at pace, financial stability risks and interconnection with the mainstream financial sector could grow. Within jurisdictions with high DeFi or crypto adoption rates, significant crypto price corrections could even reduce household wealth.

DeFi Links with CeFi Are Limited, but Crypto Links Grow

Of the meaningful USD1.7 trillion network value of crypto assets as at end-January 2022, banks' and insurance companies' exposures remain de minimis, limited by a lack of regulatory acceptance, and potentially punitive treatment within solvency regimes (an updated proposal on the prudential treatment of crypto assets is expected in mid-2022 from the Basel Committee on Banking Supervision).

However, funds focused on crypto assets held about USD50 billion in 2021, according to the Bank of International Settlements (BIS), which includes Canadian Greyscale's various crypto asset investment vehicles (holding in excess of USD34 billion as of end-January 2022). Unknown amounts are also held by family offices and by individuals.

Non-cash exposure is available within mainstream exchanges, e.g. bitcoin futures are traded on the Chicago Mercantile Exchange, and bitcoin exchange-traded funds have been approved in Canada and the US. Germany has permitted certain German funds reserved for institutional investors to invest up to a fifth of their assets in cryptocurrencies. Although not specifically linked to DeFi, these developments signal that institutional interest in digital assets is increasing.

Stablecoins Aids DeFi and Links into Centralised Finance

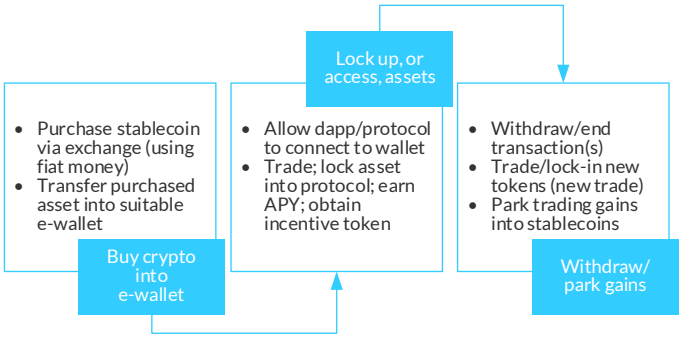
Stablecoins are popular in DeFi as most are exposed to significantly less price volatility risk than other digital assets such as ETH or BNB. Stablecoins facilitate value transfers across the mainstream financial system into DeFi, and between users, protocols and networks by using blockchain networks (thereby bypassing bank-reliant payment rail systems). Stablecoins are also used as a way to park volatile trading gains or token rewards without having to convert back into fiat currencies, and to gain income through lending on DeFi protocols (see below).

By facilitating the interchange of fiat currencies with a theoretically stable digital token widely accepted within DeFi, stablecoins act as an interconnection between the DeFi ecosystem and mainstream centralised financial systems. Fiat currencies received by stablecoin issuers may impact commercial banks' liabilities as deposits or from investment in certificates of deposit. Alternatively, stablecoin issuers may purchase commercial paper or short-dated government securities.

Because of these linkages, the USD170 billion stablecoin sector (value of top ten stablecoins at end-January 2022) is increasingly attracting the attention of regulators as a potential contagion channel for spillover risks from the digital asset ecosystem to impact the mainstream financial system (see Stablecoins Could Pose New Short-Term Credit Market Risks).

Typical Steps to Executing a Transaction Within DeFi

DeFi Ecosystem - Typical Steps to Executing a DeFi Transaction



Source: Fitch Ratings

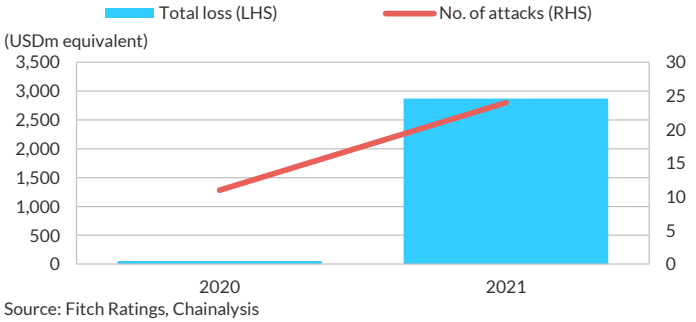
DeFi Risks Within the Ecosystem Are Broad

Cybercrime, Market Manipulation

Cybercrime targeting the digital asset space resulted in more than USD7.7 billion of assets taken from victims worldwide (source: Chainalysis), an 81% increase from 2020, as more users were drawn into the hype surrounding soaring token values and apparently attractive sources of passive income. The scale of potential fraud for this nascent sector can be regarded as a source of reputational risk. Within the DeFi ecosystem users are pseudonymous, transactions cannot be reversed (although they can all be tracked on the public blockchain), and transactions may be linked to non-custodial wallets that are not necessarily tied to individuals.

"Rug pulls" or exit scams represented the fastest growing source of fraud, accounting for 37% of all digital asset fraud revenue in 2021, versus just 1% in 2020, and have emerged as the go-to scam within the DeFi space. Rug pulls convince users to place funds into a seemingly legitimate DeFi token or DeFi service, only for funds to be drained by the developers behind the project, who then disappear. For instance, the AnubisDAO scam in October 2021 resulted in USD58 million stolen within 20 hours of a new token being issued.

Cryptocurrency Stolen in Rug Pulls, 2021 vs. 2020



Source: Fitch Ratings, Chainalysis

Risks stemming from market manipulation are another growing element of the DeFi ecosystem. Flash loan attacks, where participants use significant liquidity obtained via a flash loan to temporarily manipulate the prices of currency pairs, are on the rise. For example, in May 2021 asset prices were manipulated at the Pancake Bunny yield farming protocol, resulting in an estimated USD3 million profit after repayment of the loan. Flash loan attackers are rarely caught, as they do not leave traces, and in any case, identities can be obfuscated.

So-called "front running" attacks take advantage that miners tend to profit maximise and add transactions based on the highest fees received, rather than the order of the transactions received – analogous to the advantage obtained in high-frequency trading by users with a faster data connection. This means users can front-run a buy or sell order on an exchange that they can see is about to happen (as trades are publicly broadcast), and net a profit ahead of other participants by incentivising miners to accept their trade first.

DeFi Users Have to Manage Wallet Security Risks Directly

The security of cryptographic keys that secure wallets and ultimately assets is a point of vulnerability for users of dapps, and centralised services running on blockchain networks. Phishing incidents exploit this vulnerability, with unsuspecting victims being persuaded to part with private keys for their hot wallets, or being directed to phishing websites that mimic legitimate DeFi services and protocols, only to lose assets once they attempt a transaction removing assets to another address (and then transferred into subsequent wallets to reduce the chance of recovery). DeFi users have to manage such risks directly, whereas more centralised digital asset service providers can shoulder some responsibility for security. The use of multi-layered authentication techniques is subsequently increasing, such as requiring multiple signatures.

Absence of Anti-Money-Laundering Checks

The prevention of illicit activities and money laundering is difficult given the general absence of KYC or AML checks on dapps or protocols. Incorporating such checks is not problematic from a purely technical standpoint, and the use of shared ledgers and smart contracts could even aid operational efficiency.

However, adding KYC and AML checks poses a steep challenge to DeFi mainstreaming, as these controls will continue to be an area of maximal interest to regulators and other authorities, while being conceptually antithetical to a central pillar of DeFi. Furthermore, in contrast to new token offerings on centralised exchanges, issuance via decentralised exchanges is generally not subject to oversight or enforcement from most securities regulators (even where the issuance of tokens can be regarded as a securities offering, and therefore in scope of existing legislation).

High Market and Liquidity Risks, but Low Settlement Risk

It is not feasible to use fundamental analysis to determine market valuations within digital assets, with pricing driven by speculation, promoter visibility and narratives (including rumours). It is possible for the value of tokens to drop to zero, not due to cybercrime, but due to a change in sentiment – particularly if there is no substantial use case or fees generated by use that are shared with token holders. Consequently, the lack of an anchor to fundamentals drives extreme price volatility in digital assets, which can be magnified by thin liquidity for less well known and held tokens. This in turn can lead to significant market and liquidity risks for DeFi participants. However, settlement risks are substantially reduced by the on-chain settlement of dapps and protocols (on the same blockchain network).

Liquidity farming, i.e. encumbering tokens within liquidity pools in return for fees, can expose liquidity providers to losses arising from the price of token changing when they withdraw their token from the liquidity pool, compared to when the tokens were first deposited in the pool, termed "impermanent loss". Pools containing assets that trade within a relatively narrow corridor – for instance, stablecoins – generally result in smaller impermanent risks than more volatile tokens.

"Slippage" risks arise from latency on blockchain networks as the price difference between when a user submits a transaction to an exchange, and when the transaction is confirmed on the blockchain. Although it can be as low as a few bps on a given transaction, it can steeply increase during high trading volumes to 3%-8% of the transaction or more. Although more recent blockchain networks appear to be less prone to latency issues than for instance the Ethereum Network, risks of this nature underline the limited benefits of DeFi over traditional finance for most non-speculative users.

Interconnectivity Worsens Liquidation, Contagion Risks

Although the DeFi and crypto ecosystem appears to be largely self-contained, lessons from earlier financial crises point to the dangers of greater interconnectedness allied to excessive leverage and asset encumbrance. The lack of regulatory oversight within the digital asset space, and the speed and leverage of DeFi protocols, allied to automated liquidation triggers, make the DeFi ecosystem prone to vicious flash crashes in asset prices.

An initial drop in crypto token price can trigger the liquidation of collateral from unpaid loans – which is the main backstop available in dapps. In the absence of a lender of last resort, and no manual intervention to prevent a downward spiral in asset prices, lenders are incentivised to perform prompt liquidations, albeit at the cost of incurring losses for the borrowers.

The inherent composability and interlinkage of DeFi protocols (e.g. loan borrowings are often linked to leveraged trading and liquidity transactions), make it possible for dramatic fluctuations in digital asset prices to trigger further rounds of volatility and forced liquidations in other protocols. For instance, there was significant liquidation activity on 9 January 2022, exceeding USD340 million, when bitcoin declined below USD40,000 and other tokens fell in unison. Similar price plunges from November 2021 to January 2022 were exacerbated by forced liquidations from DeFi lending protocols.

Partly in response to the automaticity of liquidation price spirals, more recent updates to lending protocols, e.g. AAVE V2, allocate a share of the protocol's interest to a reserve factor, analogous to capital held by banks for losses, that is calibrated to the relative riskiness of a given asset based on price volatility. This reserve factor is used to protect against the protocol's solvency risk, i.e. from unpaid bad loans.

Ultimately, however, users remain responsible for setting crucial overcollateralisation and liquidation thresholds to protect themselves from price volatility risks. In the absence of a central authority overseeing and providing a coordinated backstop, there is no mechanism or human override to prevent deep price spirals that can destabilise the digital asset sector.

As the DeFi ecosystem becomes more mature, further private backstops are likely to be implemented. However, this may not be sufficient to prevent a damaging rout in crypto asset prices, which, if and when the DeFi sector becomes sufficiently material and links to mainstream finance grow (principally via stablecoins and institutions cash and synthetic crypto holdings), may fan out into the mainstream financial sector and lead to greater financial stability risks.

Bugs in Smart Contracts and Codes: Audits and Bounties

The technical complexity and the relative immaturity of the DeFi market increases the likelihood of significant vulnerabilities linked to coding issues and bugs. Smart contracts are not record keeping mechanisms that are designed for parties to easily review, but are software that automate the provision of services and actions.

The open-source architecture of DeFi protocols means that conscientious developers can sweep the relevant software codes for bugs. However, small errors or weaknesses may still reside within the protocols that can be exploited by hackers. This risk can affect any DeFi protocol, and due to the interlinkage of DeFi protocols, may expand the points of attack available to beyond the protocol with the specific issue.

Users of protocols can reduce some risk by ensuring the DeFi protocol or project has been audited by reviewing published documentation. The more reputable DeFi protocols tend to have their code and updates regularly audited by third-party specialist firms. While code audits of this kind do not guarantee that the code is entirely free from error, they can reduce the risks. In addition, developers behind protocols usually offer bounties or rewards to third-party developers who find bugs that could be exploited by criminals.

Slashing Risk for Validators of Proof of Stake Blockchains

Validators in proof of stake (PoS) blockchains face the risk the value of their encumbered token is "slashed" or permanently reduced in value, to account for any uptime violations (e.g. the computer is offline), dishonest validations, or any other malicious actions (e.g. an attempt to sign two blocks into the same blockchain location).

The slashing of holdings is intended to incentivise the availability of validators, to ensure "honest" network participation, and to promote security. Slashing penalties vary by network, and can range from being charged a fixed number of tokens, a fixed percentage, a complete slashing of the staked tokens, or the suspension or banning of the validator from the network.

Consensus Level Attacks Highlight DeFi Control Risks

Although DeFi control structures are viewed as introducing greater resilience and fault-tolerant redundancy into a system, blockchain networks' consensus mechanisms remain theoretically vulnerable to criminal attempts to wrestle control for a short duration, known as "51% attacks".

This refers to a situation where one or more malicious actors collude to command at least 51% of the network's computing power. Once the blockchain network is under their effective control, the criminals can confirm invalid transactions, i.e. double-spend on tokens, or seek to reverse transactions. As executing a 51% attack is expensive across large networks such as Ethereum, these attacks tend to occur on smaller and more centralised proof of work (PoW) blockchain networks, e.g. Bitcoin SV in July 2021, Bitcoin Gold in 2020.

On PoW consensus networks a 51% attack would involve harnessing massive computing power, which would require upfront funding solely in terms of electricity costs (costs could exceed a million dollars – based on estimates for a one-hour attack on PoW blockchains, courtesy of www.crypto51.app). Whereas in PoS networks, an attacker would have to accrue over 51% of the network's total circulating tokens. Reversal of the attacks on either type of blockchain network would be feasible, but would likely involve a so-called "hard fork" in the version of the blockchain (and related token), comprising those users who approve the rollback, versus those who do not agree with the rollback.

Regulating DeFi Without Stifling Innovation

Authorities Are Trying to Understand the Nascent Sector

Amid the rapid evolution and market growth of digital assets, authorities appear to be trying to review and make sense of DeFi, which has only really scaled up in 2021 and will continue to grow and develop (although growth in DeFi does appear to have slowed more recently). Regulators' attention has focused on the implications of systemic stablecoins (see Stablecoins: Regulatory Approaches and Credit Considerations for more details), which facilitate value transfers between mainstream finance and the DeFi ecosystem.

In its December 2021 Quarterly Review, the BIS warned that the growth of DeFi poses financial stability concerns, due to its vulnerabilities, such as high leverage, stablecoins' potential liquidity mismatches, and the inherent interconnectedness of DeFi. These risks, the BIS argues, are exacerbated within DeFi by the absence of public backstops and shock absorbers in the ecosystem, that regulated financial institutions enjoy.

In terms of regulation for the sector, the BIS notes the inherent practical difficulties of exercising oversight, given that there are practical ways that users may evade controls or bans on engaging with DeFi services (e.g. using VPNs, foreign bank accounts or payment cards). Nevertheless, the BIS recommends public authorities' use DeFi's more centralised DAO stakeholder arrangements and governance protocols to contain DeFi-related issues before the ecosystem attains systemic importance. The BIS added that regulatory safeguards would also help to ensure that the innovative potential of DeFi brings overall benefits to finance.

The exclusive use of software will likely require authorities to develop specific tools to review, for example, smart contracts, and appropriate skilled persons to undertake code audits, for instance. Many authorities' have used so-called regulatory "sandboxes" to provide firms – usually fintechs – with the ability to test products and services within a controlled environment, where the regulators support developers to identify appropriate user protection safeguards to build into new products and services. As all DeFi protocols are first initiated under the control of a single (centralised) development team, it may be possible for regulators to actively reach out to, and participate with, software development teams with interests within the DeFi space, to better understand the nascent industry and the opportunities and risks.

Finding the Responsible Team or Authority Is Difficult

Existing regulatory regimes are more readily applied to mainstream financial services providers, typically incorporated as body corporates, with a registered physical address within a given jurisdiction, making it easier to identify the loci of responsibilities.

This approach is difficult to apply within DeFi. Dapps and the underlying protocols are borderless, immensely complicating consumer safety, as well as the application of authorities' rules and regulations, which are jurisdiction-based. Smart contracts are not associated with a given user but rather interact with wallets and thus assets of a user. The original developers behind a protocol may no longer be responsible for deploying the protocol across dapps, may lack the ability to modify DeFi services, or may no longer be in charge of governance decisions.

The more mature protocols tend to hand more control to a so-called decentralised autonomous organisation or DAO, which may be regarded as an association suitable for authorities' focus, albeit it often lacks a legal personality and location (see *Annex*). Even where jurisdictions' legal frameworks can facilitate DAOs to adopt a legal structure, for instance as a public foundation, token holders may reject such a prospect, as it may be regarded as being antithetical to the philosophy of DeFi. However, there are a growing number of examples where development teams or DAOs behind widely used protocols, e.g. AAVE and Nexus Mutual, have opted to organise under an incorporated entity with a registered office and nominated officers.

To date, regulatory enforcement actions have tended to focus on individuals who promote and market DeFi projects, including new token offerings (for example, the US SEC action in August 2021), and the strengthening of rules on digital asset marketing and guidelines (as unveiled in Spain, the UK and Singapore).

Regulation of Wallets and Fiat Currency Touchpoints

The regulation of users' wallets and touchpoints with fiat currency payments is a focal point for authorities, given the potential of DeFi to undermine AML requirements and facilitate financial crime. Existing regulatory regimes require the application of KYC and AML requirements when transferring fiat currencies into private wallets, and pressuring institutions involved in fiat currency payments to conduct appropriate checks before permitting transfers into digital wallets.

Global guidance on this topic was first issued by the Financial Action Task Force in June 2019 (itself modelled on the US Bank Secrecy Act requirements), which stated that jurisdictions should ensure that virtual asset service providers "obtain and hold required and accurate originator (sender) information and required beneficiary (recipient) information", i.e. information relating to private wallets.

Enforcement of these rules is possible for wallets issued by centralised firms, which are often registered as licensed money transmitters or as electronic payment institutions. However, it is far harder for authorities to enforce requirements against DeFi wallet providers.

Jurisdictional Approaches Vary

Since May 2021, China has imposed an extensive ban on virtually all digital asset trading and issuance of private tokens, including stablecoins, ahead of issuing its own central bank digital currency, the e-CNY, which was trialled in February 2022 by domestic and international users for the Winter Olympics. The People's Bank of China (PBoC) reiterated in a notice that all related transactions are regarded as illicit financial activities, which would appear to ban the use of DeFi services by Chinese citizens. In addition, the PBoC forbids foreign exchanges from providing services to China-based investors, and forbids local banks, payment companies and internet firms from facilitating cryptocurrency trading nationally.

In January 2022 the Central Bank of Russia issued consultative proposals, which, if enacted, would ban the trading of cryptocurrencies for fiat currency in Russia, as well as banning the use of Russia's financial infrastructure for cryptocurrency operations. The issuance (including mining), circulation or exchange of cryptocurrencies would be prohibited, and local banks would be banned from investing in cryptocurrencies. On the surface, this approach could ban Russians from using DeFi services, if enacted (see Proposed Russian Crypto Ban Eases Risks, but May Curb Innovation).

Authorities in Hong Kong, India and Indonesia appear a little more nuanced than in China, preferring to regulate the use of digital assets akin to a commodity and not permitting their use for payments. The authorities appear to be an early stage of assessing the risk implications of DeFi, which includes calling for advice, and reflecting on the recently published views of the BIS.

In Singapore, centralised digital asset services are regulated under the Securities and Futures Act (SFA), and tokens and wallets under the Payment Services Act, which came into force in January 2020 to regulate payment services such as e-wallets. Decentralised exchanges are theoretically scoped in as an "organised market" under the SFA, and require approval or recognition from the Monetary Authority of Singapore (MAS).

Existing pan-EU rules on digital assets relate mainly to the AML regime. The EU Commission's proposed Markets in Crypto-Assets Regulation (MiCA) seeks to regulate the issuance of digital assets (excluding tokenised securities, which are already covered under existing legislation). Once adopted and in force, which could be as early as 1H22, MiCA will set out rules, licensing, prospectus and disclosure requirements for centralised use cases of digital assets. However, it appears that DeFi-related applications and use cases do not neatly fit into MiCA, which was largely drafted before DeFi came to the attention of the authorities.

In the US, multiple federal authorities appear to have jurisdiction over aspects of DeFi through existing regimes. In particular, the SEC recently proposed changes to the definition of an exchange as those that "make available . . . communication protocols" through which "buyers and sellers can interact and agree to the terms of a trade" – which could include DeFi exchanges. However, as there is not yet a bespoke legal and regulatory framework for digital assets, federal regulation of digital assets remains fragmented and unclear.

The 2021 Digital Asset Market Structure and Investor Protection Act proposed by Democratic Representative Don Beyer represents one of the most comprehensive efforts in creating a regulatory framework and greater definitional clarity for digital assets. Guidance has been issued by bank supervisors concerning the issuance of stablecoins, and the use of blockchain-related technologies.

Regulated 'DeFi 2.0' May Emerge from Unregulated DeFi

The DeFi sector has been characterised by rapid change, with protocols continually updated. Despite the lack of regulatory oversight, there is evidence of self-regulation as protocols evolve, with popular dapps incorporating safeguards, and in some cases complying with local regulatory and licensing requirements.

The reserves within the AAVE lending platform appear to mimic elements of the historical Basel I capital adequacy prudential framework for banks. A permissioned liquidity pool protocol has been launched for institutions, requiring users to comply with KYC/AML requirements, and is authorised by UK regulators. Nexus Mutual's insurance-like service is backed up by a solvency reserve based on elements of the EU's regulatory regime, and requires its users to meet KYC/AML requirements.

As regulators and users of DeFi better understand the opportunities and risks presented by DeFi, Fitch expects that a combination of supervisory guidelines and self-regulation will reduce some of the risks associated with DeFi. This could take the form of implementing basic AML and KYC checks, the refusal of access to wallets (i.e. addresses) previously associated with cybercrimes, undertaking software audits and receiving certification (as many protocols already do), and accepting location-based licensing and securities regulations (for token issuance).

However, while regulation and laws can bring security and stability to DeFi and the digital assets space, some projects may have to change their services as new rules are created. And accepting regulatory oversight may undermine the composability and interlinkage of existing DeFi protocols, meaning that some DeFi services may not be compliant.

Constraints resulting from self- or enforced regulation may eventually lead the DeFi sector to bifurcate, with a more regulated DeFi 2.0 emerging that meets authorities' requirements attracting institutional and corporate counterparties. An unregulated DeFi could continue to exist, accessed via virtual private networks and anonymous wallets, offering higher potential levels of rewards, alongside a higher assumed level of risk.

Annex – Glossary of Terms

Block: A time-stamped data structure that is used to aggregate transactions, which can be used to record transactions, for instance, asset transfers.

Blockchain: A type of distributed ledger technology which, together with other related technologies, acts as settlement layer for transactions. There are two categories of blockchains: permission-less blockchains, where any entity is able to join and leave without permission; and permissioned blockchains, which are typically composed of a group of authenticated participants. DeFi is built on top of permission-less blockchains.

Bitcoin: The first widely recognised blockchain-based digital asset, intended to be used as a unit of account and means of payment.

Digital Assets: Digital representations of value, such as tokens, which can be used for payment, trading or investment purposes, or to access a good or service.

Ethereum: A decentralised, open-source blockchain with smart contract functionality. Ether (ETH) is the native token of the platform.

Proof of Stake (PoS): A mechanism to determine which participant creates a block on a blockchain based on locked tokens being randomly selected by the protocol at specific intervals. Allows blocks to be produced without completing complex mathematical puzzles or specialised mining hardware (i.e., less energy intensive).

Proof of Work (PoW): A mechanism to determine which participant creates a block on a blockchain based on competing to solve a complex mathematical puzzle. Whoever solves it first, gets the right to add the next block to the blockchain.

Security Tokens: These function as and convey a direct interest in existing securities, such as company shares or bond securities.

Smart Contracts: Programs (stored on a blockchain) that run when predetermined conditions are met, by following simple "if/when…then…" statements or rules. They are typically used to automate the execution of an agreement without any intermediary's involvement or to automate a workflow, triggering the next action when conditions are met.

Stablecoin: A type of digital asset that has a stabilisation mechanism that at all times links its value to an underlying asset and or pool of assets, for example a fiat currency.

Staking: The process of committing crypto holdings to support the security and operations of a PoS blockchain network, in order to obtain rewards or earn interest. Staking involves validators who lock up their token (within a suitable wallet) so they can be randomly selected by the protocol at specific intervals to create a block. Participants that stake larger amounts of a given token have a higher chance of being chosen as the next block validator.

Total Value Locked: The quantum of (crypto) assets that are currently being staked in a specific protocol, i.e. as liquidity being secured by a specific DeFi application – not to be confused as representing, for instance, outstanding loans.

Wallet: An infrastructure tool used to send and receive digital assets through blockchain networks, and used to summarise asset holdings by interacting with blockchain networks. The wallet carries information comprising one or more pairs of public and private "keys", and an "address" alphanumeric identifier that functions as a location on the blockchain (generated based on the public and private keys). The private key gives access to digital assets, regardless of which wallet is used – software, hardware, and paper wallets, or hot (connected to internet) or cold (disconnected from internet) wallets.

DISCLAIMER & DISCLOSURES

All Fitch Ratings (Fitch) credit ratings are subject to certain limitations and disclaimers. Please read these limitations and disclaimers by following this link: https://www.fitchratings.com/understandingcreditratings. In addition, the following https://www.fitchratings.com/rating-definitions-document details Fitch's rating definitions for each rating scale and rating categories, including definitions relating to default. Published ratings, criteria, and methodologies are available from this site at all times. Fitch's code of conduct, confidentiality, conflicts of interest, affiliate firewall, compliance, and other relevant policies and procedures are also available from the Code of Conduct section of this site. Directors and shareholders' relevant interests are available at https://www.fitchratings.com/site/regulatory. Fitch may have provided another permissible or ancillary service to the rated entity or its related third parties. Details of permissible or ancillary service(s) for which the lead analyst is based in an ESMA- or FCA-registered Fitch Ratings company (or branch of such a company) can be found on the entity summary page for this issuer on the Fitch Ratings website.

In issuing and maintaining its ratings and in making other reports (including forecast information), Fitch relies on factual information it receives from issuers and underwriters and from other sources Fitch believes to be credible. Fitch conducts a reasonable investigation of the factual information relied upon by it in accordance with its ratings methodology, and obtains reasonable verification of that information from independent sources, to the extent such sources are available for a given security or in a given jurisdiction. The manner of Fitch's factual investigation and the scope of the third-party verification it obtains will vary depending on the nature of the rated security and its issuer, the requirements and practices in the jurisdiction in which the rated security is offered and sold and/or the issuer is located, the availability and nature of relevant public information, access to the management of the issuer and its advisers, the availability of pre-existing third-party verifications such as audit reports, agreed-upon procedures letters, appraisals, actuarial reports, engineering reports, legal opinions and other reports provided by third parties, the availability of independent and competent third- party verification sources with respect to the particular security or in the particular jurisdiction of the issuer, and a variety of other factors. Users of Fitch's ratings and reports should understand that neither an enhanced factual investigation nor any third-party verification can ensure that all of the information Fitch relies on in connection with a rating or a report will be accurate and complete. Ultimately, the issuer and its advisers are responsible for the accuracy of the information they provide to Fitch and to the market in offering documents and other reports. In issuing its ratings and its reports, Fitch must rely on the work of experts, including independent auditors with respect to financial statements and attorneys with respect to legal and tax matters. Further, ratings and forecasts of financial and other information are inherently forward-looking and embody assumptions and predictions about future events that by their nature cannot be verified as facts. As a result, despite any verification of current facts, ratings and forecasts can be affected by future events or conditions that were not anticipated at the time a rating or forecast was issued or affirmed.

The information in this report is provided "as is" without any representation or warranty of any kind, and Fitch does not represent or warrant that the report or any of its contents will meet any of the requirements of a recipient of the report. A Fitch rating is an opinion as to the creditworthiness of a security. This opinion and reports made by Fitch are based on established criteria and methodologies that Fitch is continuously evaluating and updating. Therefore, ratings and reports are the collective work product of Fitch and no individual, or group of individuals, is solely responsible for a rating or a report. The rating does not address the risk of loss due to risks other than credit risk, unless such risk is specifically mentioned. Fitch is not engaged in the offer or sale of any security. All Fitch reports have shared authorship. Individuals identified in a Fitch report were involved in, but are not solely responsible for, the opinions stated therein. The individuals are named for contact purposes only. A report providing a Fitch rating is neither a prospectus nor a substitute for the information assembled, verified and presented to investors by the issuer and its agents in connection with the sale of the securities. Ratings may be changed or withdrawn at any time for any reason in the sole discretion of Fitch. Fitch does not provide investment advice of any sort. Ratings are not a recommendation to buy, sell, or hold any security. Ratings do not comment on the adequacy of market price, the suitability of any security for a particular investor, or the tax-exempt nature or taxability of payments made in respect to any security. Fitch receives fees from issuers, insurers, guarantors, other obligors, and underwriters for rating securities. Such fees generally vary from US$1,000 to US$750,000 (or the applicable currency equivalent) per issue. In certain cases, Fitch will rate all or a number of issues issued by a particular issuer, or insured or guaranteed by a particular insurer or guarantor, for a single annual fee. Such fees are expected to vary from US$10,000 to US$1,500,000 (or the applicable currency equivalent). The assignment, publication, or dissemination of a rating by Fitch shall not constitute a consent by Fitch to use its name as an expert in connection with any registration statement filed under the United States securities laws, the Financial Services and Markets Act of 2000 of the United Kingdom, or the securities laws of any particular jurisdiction. Due to the relative efficiency of electronic publishing and distribution, Fitch research may be available to electronic subscribers up to three days earlier than to print subscribers.

For Australia, New Zealand, Taiwan and South Korea only: Fitch Australia Pty Ltd holds an Australian financial services license (AFS license no. 337123) which authorizes it to provide credit ratings to wholesale clients only. Credit ratings information published by Fitch is not intended to be used by persons who are retail clients within the meaning of the Corporations Act 2001.

Fitch Ratings, Inc. is registered with the U.S. Securities and Exchange Commission as a Nationally Recognized Statistical Rating Organization (the "NRSRO"). While certain of the NRSRO's credit rating subsidiaries are listed on Item 3 of Form NRSRO and as such are authorized to issue credit ratings on behalf of the NRSRO (see https://www.fitchratings.com/site/regulatory), other credit rating subsidiaries are not listed on Form NRSRO (the "non-NRSROs") and therefore credit ratings issued by those subsidiaries are not issued on behalf of the NRSRO. However, non-NRSRO personnel may participate in determining credit ratings issued by or on behalf of the NRSRO.