KEY POINTS

- Decentralised Finance (DeFi) facilitates peer-to-peer transactions without a centralised party, instead relying on code-based solutions to provide financial services to a wider pool of users.
- However, DeFi also has its own associated risks such as technological hacks, and the risk of abuse for money laundering and terrorism financing. The question of *who* should bear responsibility for the operations of a DeFi application also creates difficulties with regulating DeFi applications.
- Recognising that most DeFi applications lack a central operating entity, regulators are seeking to impose regulatory obligations on a wider class of persons, which could include the creators and controllers of DeFi applications, as well as persons who profit off such DeFi applications.

Feature

Authors Elaine Chan and Sion Yoong Tian

Decentralised finance (DeFi): a game-changer or just a passing fad?

DeFi is a term used to describe decentralised applications that provide financial services using blockchain technology. DeFi leverages on technologies such as smart contracts and open-source protocols to execute peer-to-peer transactions without the use of any centralised party. Given the increasing prevalence and receptiveness towards DeFi, stakeholders in the financial industry should possess some basic understanding of this new alternative to the traditional financial system. This article outlines the distinctive characteristics, underlying benefits and risks of DeFi applications, and the regulatory approaches towards regulating such applications.

OVERVIEW OF THE DEFI LANDSCAPE

As Decentralised finance (DeFi) does not rely on traditional centralised financial intermediaries or institutions for the execution of financial services, proponents have described DeFi as an alternative financial system which is built for the Internet age. Participants can freely access payment and financial solutions offered by DeFi platforms – so long as they have internet access and a cryptocurrency wallet. Many DeFi applications also adopt a decentralised governance model, where tokenholders wield control and decision-making powers over the DeFi application's parameters through voting.

CHARACTERISTICS OF DEFI

DeFi is broadly distinguished from traditional financial services in the following key aspects:

- no intermediary involvement;
- greater accessibility;
- non-custodial nature; and
- open and transparent systems.

No intermediary involvement

The operations and settlement of DeFi transactions happens entirely on a blockchain, executed by open-source code and smart contracts which consist of pre-determined and automated rules programmed into the DeFi application. As such, transactions do not require participants to rely on a centralised intermediary (eg a broker or a bank) to execute transactions. This is also known as the "trustless" nature of DeFi.

Greater accessibility

DeFi applications are generally accessible to anyone who has an internet connection and a cryptocurrency wallet. There are typically no restrictions as to the type of persons who may access the financial services provided by DeFi applications. This is also known as the "permission-less" nature of DeFi.

In contrast, a person's access to traditional financial services is often restricted by various factors. For example, traditional financial institutions may examine a borrower's credit score, salary, employment and bankruptcy information during a loan application. On the other hand, borrowers using a DeFi lending protocol are simply required to over-collateralise their loans, rather than pass a credit score or employment background assessment.

Non-custodial nature

DeFi applications generally allow users to retain control over their digital assets, through their own personal blockchain wallets connected to the DeFi application. Even when users lock up or stake their cryptocurrencies on a DeFi application, there is no centralised entity that has control or custody over these "locked up" digital assets. Rather, the users' digital assets are only subject to the rules encoded into the DeFi application's smart contracts, which determine the time period in which a user's tokens may be locked-up or released. In contrast, for traditional financial institutions, customer funds are usually subject to the control and custody of the financial institution.

Open and transparent systems

DeFi applications are typically open-source protocols, meaning that anyone can view and verify the application's code and protocol rules directly. This enhances the transparency of DeFi applications, as participants can readily verify the integrity and security of the system.

BENEFITS OF DEFI

Proponents of DeFi believe that DeFi's unique characteristics give it an edge over centralised finance. As a starting point, DeFi's trustless and fully automated nature could result in faster and more efficient transactions, as the execution and performance of transactions are solely based on the protocol's pre-programmed code. Such reliance on a code-based solution to execute transactions arguably enhances both

Feature

Biog box
Elaine Chan is the Joint Head of the Financial Services Regulatory Practice at WongPartnership LLP. She is a specialist in Financial Services Regulatory, Compliance and Governance and advises financial institutions on regulatory, licensing, compliance, governance and transactional matters. Email: elaine.chan@wongpartnership.com

consistency and reliability in transaction execution, where participants no longer have to rely on traditional intermediaries to carry out their orders.

For example, decentralised exchanges (DEX) and automated market makers (AMM) enable participants to buy, sell or swap various digital tokens and assets without the need for intermediaries. DEXs and AMMs distinguish themselves from conventional exchanges and market makers by doing away with centralised intermediaries such as brokers, custodians and clearing houses to provide its exchange services. Through an order book model, buyers' and sellers' orders in relation to digital assets are automatically matched by the DEX protocol, with no intermediary involvement. Alternatively, under an AMM model, participants can trade against the DeFi protocol itself, by contributing their digital assets to a liquidity pool controlled by the DeFi protocol.

DeFi's accessibility has also been touted as the solution to the perceived inefficiencies and structural inequalities of the traditional financial system. It is proffered that DeFi provides a wider group of persons with accessibility to financial services, who would otherwise have been excluded from access to traditional financial services due to geographical constraints or their credit or employment background.

As an illustration, a popular DeFi use case – DeFi lending applications, typically involve liquidity providers who contribute digital assets to a liquidity pool on a blockchain. Such liquidity providers mirror the role of depositors in traditional banking. By contributing to the liquidity pool, liquidity providers may then receive interest payments, which are determined algorithmically based on the borrowing demand and lending supply of the underlying digital asset. Unlike traditional lending undertaken by centralised financial institutions, decentralised lending applications do not conduct any credit assessment on its borrowers. Rather, a borrower's credit risk is mitigated through other means, for example, by requiring borrowers to over-collateralise their loans.

Furthermore, DeFi's non-custodial design, which allow participants to retain custody over their digital assets, could reduce the risk of their funds being mishandled by intermediaries, or be subject to the risk of an intermediary's insolvency.

Lastly, DeFi's open and transparent architecture allows for the DeFi applications' code to be taken and adapted to create new DeFi applications. This not only facilitates interoperability, but also promotes competition among DeFi applications. This differs from the traditional financial system, where market power may be concentrated within a small circle of incumbent financial institutions, which may indirectly stifle the growth of new players or innovative practices in the financial industry.

RISKS AND CONCERNS OF DEFI

DeFi is not without its set of challenges. Notwithstanding the benefits that DeFi stands to bring to the financial services industry, it should be borne in mind that DeFi is still a relatively new concept, which comes with its attendant risks and challenges. DeFi's significant uptake in recent years has been coupled with a spate of significant technical failures and hacks on DeFi platforms. Important questions also remain as to whether DeFi applications are becoming vehicles for fraud and illicit activity due to the inherent difficulty of regulating an application that has no central entity to impose liability and responsibility on.

In order to gain the trust of players in the broader financial sector, it would be imperative to have answers to some pressing questions associated with DeFi, so that such risks can be mitigated. Some of the pressing questions and key risks generally associated with DeFi are set out below.

Technical risks

Technical risk arises out of most types of technologies. Specific to DeFi, is the risk that the underlying smart contracts that the DeFi application runs on could be subject to hacks and coding errors. While DeFi's non-custodial design may reduce the risk of a central party mishandling users' funds, DeFi users are still vulnerable to loss of funds through third-party hacks. Given the immutability and irreversibility of transactions settled on a blockchain, losses arising from false transactions entered into using a DeFi application would typically be permanent. In an effort to address these technical risks, certain DeFi applications offer "bounty rewards" for users who have spotted and reported bugs to the DeFi application.

Challenges in attributing responsibility

As a trustless system, governance and decision making on DeFi applications are typically decentralised. However, the lack of a centralised operating entity brings about the question of *who* should bear responsibility and accountability for the operations of the DeFi application. Where a DeFi application adopts a decentralised governance model, it is not only unclear as to who should bear ultimate responsibility for the governance and running of the application, but also how responsibility should be allocated. For example, in the event that an error in the DeFi application's code results in a security breach and a loss of user funds, should responsibility be attributed to the programmer, who simply operationalises the changes that have been agreed upon by the tokenholders of the DeFi application, or some other party altogether?

Separately, if the governance tokens of a DeFi application are held by a small group of associates who act in concert, should this small and potentially ascertainable group of tokenholders be held accountable for their decisions made in respect of the DeFi application?

Money laundering and financing of terrorism risks

Due to the permission-less nature of DeFi applications, DeFi applications may be used by bad actors to conduct illicit activities such as money laundering and terrorism financing (ML/TF). Transactions on DeFi applications may be difficult to regulate with traditional anti-money laundering and countering the financing of terrorism (AML/CFT) controls, such as transaction monitoring and customer due diligence requirements. This is because there is often no centralised entity that regulators can impose requirements on to implement such controls, and users are

Biog box

Sion Yoong Tian is a partner in the Financial Services Regulatory, the Derivatives & Structured Products and the FinTech Practices. His main practice areas are financial services regulatory, FinTech, blockchain, and derivatives and structured products (both transactional and regulatory). Email: sionyoong.tian@wongpartnership.com

identifiable only by their cryptocurrency wallet addresses.

Moreover, given the decentralised governance model of DeFi applications, it may be harder for compliance and regulatory requirements to be implemented. A situation may arise where the tokenholders of a DeFi application may decide to vote against certain compliance updates that could be important in preventing DeFi applications from being used by dishonest actors. Under such circumstances, the issue of allocation of responsibility of the governance of DeFi applications comes to the forefront again.

APPROACHES TO REGULATING THE DEFI SPACE

As the blockchain and crypto space evolves, efforts have been made at both an international and national level to introduce new laws or guidance to regulate blockchain and cryptocurrency activities. However, the fundamental question of *who* should bear responsibility for ensuring compliance with regulatory obligations remains a central issue in the regulation of the DeFi space. We set out below an overview of the regulatory approaches adopted by the Financial Action Task Force (FATF) and Singapore in addressing the challenges introduced by DeFi.

International standard setting bodies on DeFi

The FATF is an inter-governmental body that develops global standards for AML/CFT. In October 2021, the FATF released its updated Guidance on the application of the risk-based approach towards regulating virtual asset (VA) activities and the operations of Virtual Asset Service Providers (VASP). VASPs are persons that carry on a business in relation to the: (i) exchange of VAs and/or fiat currencies; (ii) safeguarding or administration of VAs; (iii) transfer of VAs; and (iv) provision of financial services related to an offer and/or sale of a VA.

Under FATF's Guidance, DeFi applications are not considered as VASPs, because the FATF standards are not intended to apply to the "underlying software or technology". However, persons that "maintain control or sufficient influence" (for example through having the power to set or change the DeFi platform's parameters or being able to profit from the platform's operations), such as the platform's creators, owners or operators, may nevertheless be regarded as VASPs. Consequently, FATF appears to have adopted a more expansive approach to determining *who* should bear responsibility for implementing AML/CFT obligations in respect of DeFi platforms. While the creators or developers themselves may not execute the DeFi services (which is carried out through program codes), they may nevertheless still exert significant control or influence over the governance of such DeFi protocols.

Singapore's regulatory regime concerning digital tokens

In Singapore, the regulatory approach towards digital tokens is determined by two overarching factors: (i) the nature of the digital tokens; and (ii) the type of activities conducted in respect of these digital tokens. One important piece of legislation is the Payment Services Act 2019 (No. 2 of 2019) (PSA). This legislation regulates, among others, service providers who deal in or facilitate the exchange of digital tokens that are characterised as "digital payment tokens" (DPTs). As part of the PSA regulatory framework, MAS also prescribes certain AML/CFT requirements which take into account the inherently higher ML/TF risks posed by DPTs. Further amendments to the PSA are currently underway, which are intended to align the PSA with the revised FATF standards to address ML/TF risks posed by VASPs that are not already regulated as financial institutions. This includes expanding licensing obligations to include persons who: (i) facilitate the transfer of DPTs; (ii) provide custodial wallet services for DPTs; and (iii) facilitate the exchange of DPTs, without coming into possession of money or DPTs.

Beyond the PSA, if digital tokens are not considered DPTs, they could alternatively be regulated as financial products under other regulatory regimes (eg as a security or unit in a collective investment scheme), depending on the uses, rights and benefits associated with the relevant digital token. Consequently, the DeFi services offered in relation to such digital tokens could be regulated under such regimes.

In light of the enhanced FATF standards, the MAS also intends to introduce a new Omnibus Act to regulate Singapore-incorporated entities who provide Digital Token (DT) services outside Singapore. The Omnibus Act seeks to impose licensing requirements on DT service providers who carry on business in (among others) dealing in DTs, safeguarding DTs, or facilitating the exchange of DTs. The MAS has also stated it may require DT service providers to establish and staff adequate AML/CFT compliance function in Singapore.

Currently, both the PSA and the new Omnibus Act seek to regulate persons or entities that provide DPT or DT services, and therefore it is not clear how these regulatory regimes would apply in the context of DeFi services without a centralised operating entity. It is possible that the FATF's expansive approach in regarding the creators of DeFi applications as VASPs could result in a future expansion of these regulatory regimes to expressly cover such creators. After all, whilst these DeFi creators do not physically execute the transactions on a DeFi application, they may nevertheless still exert control and influence over the medium and technology through which such transactions may be executed.

Looking forward, it is likely that international and national regulatory frameworks would have to continue to evolve in tandem with developments in the DeFi space. It would be prudent for stakeholders and participants in both the traditional and DeFi space to continue to monitor regulatory developments in this regard, as this could have an impact on how DeFi applications may be regulated in the future. ■

Further Reading:

- Financial Crime Update (2020) 7 JIBFL 496.
- Crypto comes of age? (also, DeFi, NFTs, Web3 and the metaverse) (2021) 6 JIBFL 434.
- LexisPSL: Banking & Finance: Articles: The exciting world of NFTs: a consideration of regulatory and financial crime risks.