MFSA FinSights | Enabling Innovations

Decentralised Finance ('DeFi')

The financial sector is continuously evolving through the rapid development and adoption of new technologies. The term 'FinTech' generally refers to financial innovation that seek to provide enhanced financial service offerings through the utilisation of enabling technologies. These generally include Distributed Ledger Technology & Smart Contracts; Artificial Intelligence, Machine Learning & Big Data, Cloud Computing, Web 3.0, Application Programme Interfaces and Micro-Services; Robotic Process Automation and the Internet of Things.

As part of the MFSA's initiatives to generate awareness, drive culture and deliver a cross-sectoral knowledge platform which can support the MFSA's functions in preparing for the financial services of tomorrow, these insights will delve into enabling technologies, enabling innovations and their sectoral applications.

1 What is DeFi?

Decentralised Finance otherwise known as DeFi is an emerging form of decentralised and autonomous financial services powered by Smart Contracts. DeFi facilitates unrestricted access to the disintermediated financial services akin to the traditional financial system ('TradFin') on a quasi-anonymous basis. It claims to increase the efficiency security, openness, accessibility, transparency and interoperability of financial services as compared to the traditional financial system.

In its purest form DeFi provides for a time-efficient peer-to-peer financial system that is decentralise in terms of infrastructure and governance. Decentralisation of infrastructure emanates from having a common settlement layer based on public Distributed Ledger Technology, namely, blockchain where transactions are validated by decentralised network of nodes. On the other hand, once a decentralised application[1] ('DApp') is developed and deployed on the blockchain its governance may be gradually decentralised as it may be gradually ceded to the user community. This may ultimately transform into a decentralised autonomous organisation ('DAO')[2]. The continued growth of this innovative financial sector raises questions on the functionalities, opportunities, challenges, risks by various stakeholders including the regulators and standard setting bodies such as International Organization of Securities Commissions ('IOSCO'), Organisation for Economic Co-operation and Development ('OECD'), Financial Stability Board ('FSB') and International Monetary Fund ('IMF').

2 How DeFi works

In the context of DeFi, the most notable public blockchain is Ethereum that was the first to reinvent crypto assets ecosystem by introducing new functionalities though smart contract applications. DeFi infrastructure grants everyone with 'read' and 'write' rights that ultimately result in the ability to view, interact or deploy DApps on the blockchian, by anyone with an internet connection. Decentralised Finance is integrated on a multilayer IT infrastructure that is commonly referred to DeFi Stack, as illustrated in Figure 1. The settlement, asset, protocol, application & aggregation layers are built off one another promoting an interoperable environment.

[1] DApps - software programs stored on the blockchain that run when predetermined conditions are met.
[2] DAO is essentially an organisation with decentralised governance.

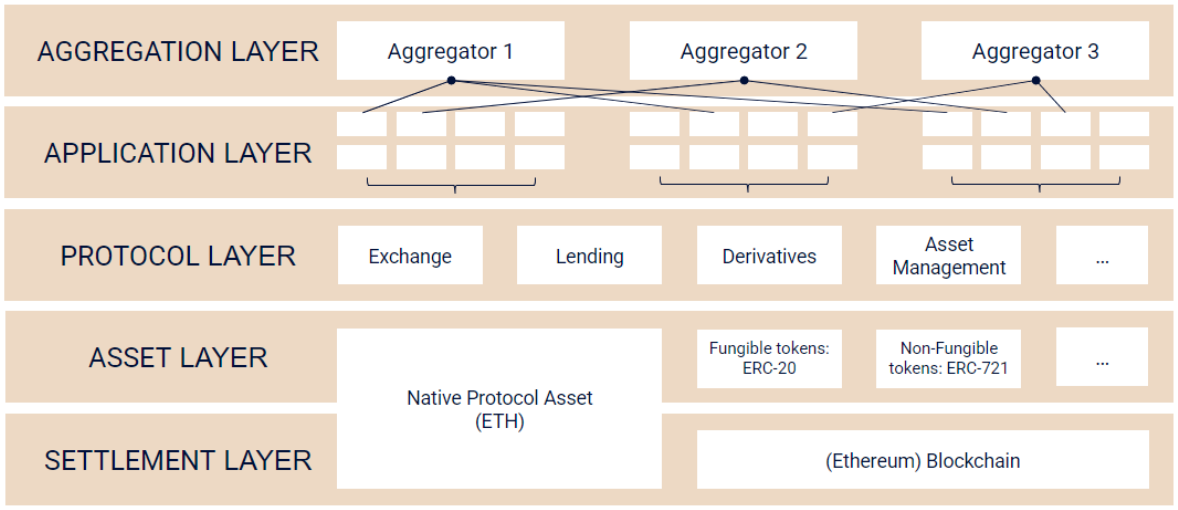

FIGURE 1: THE DEFI STACK
Source: Schaer, F. (2021), Decentralised Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review, Second Quarter 2021.

2.1 Settlement Layer

Public blockchains act as fundamental building blocks of DeFi system providing a decentralised common settlement layer for DApps and ensuring secure storage of ownership information. They are also deemed robust since they can continue to function even if some nodes are compromised, unlike their centralised counterparties.

This layer stores all transaction records in chronological order, securing them cryptographically *'as "blocks" of transactions in a "chain"'* (IOSCO 2022, p. 4), that continuously alter the state of the blockchain with every additional block. All the network activity is transparent allowing for anyone to verify the validity of transactions and the ruleset of any smart contract that is deployed on the blockchain. Finally, the common settlement layer allows for full interoperability of various DApps on the same blockchain.

In contrast to TradFin where settlement may take days, blockchain settlement may on average be concluded within seconds. Although, heavy settlement activity on the base layer may eventually affect the overall speed and validation cost of the blockchain.

2.2 Asset Layer

The Asset layer consists of tokens issued or minted on the settlement layer, which are referred to as the native tokens[3] of the blockchain itself. Numerous other tokens may be issued on the blockchain by means of smart contacts however the blockchain relies only on the native once for its functionality. The classes of tokens generally available of this layer may be split into fungible[4] and non-fungible tokens ('NFTs')[5], both of which may represent crypto assets as well as real-world assets such as financial instruments. The tokens minted on the asset layer may not only be associated to governance of DApps or DAOs but may also act as an incentive for holders to further secure the network, through the validation of transactions.

[3] Native tokens – also referred to as Native Protocol Assets
[4] Fungible tokens - are identical tokens that are freely interchangeable and are mostly issued via an ERC-20 type smart contract.
[5] NFT – is a special type of crypto asset that is unique and is not interchangeable with another crypto asset.

2.3 Protocol Layer (Smart Contact)

The third layer of the stack consists of smart contracts that enable DeFi functionalities, including amongst others, disintermediated trading, lending, derivatives, investment and insurance services on the blockchain. The open-source code of smart contracts stimulates innovation and creativity in decentralised financial services whereby new functionalities and incremental improvements are introduced from the existing protocols. Finally, by having the same settlement layer it enables DeFi protocols to be composable[6], resulting in creation of new and complex financial products.

2.4 Application & Aggregation Layers

This layer is a user-friendly web-based interface that provides for a seamless user interaction with the underlying DeFi protocols. An interface may be both protocol-specific & protocol-agnostic. The former facilitates user's interaction with a single protocol while the latter (aggregator) enables the combined use of several DApps at once through a single User Interface ('UI'). The aggregation layer can serve as a comparison tool of DApps to optimise user's returns or achieve specific investment exposure objectives. Also, in the context of best execution, aggregators may sub-divide a transaction and execute it on several different protocols to ensure the best terms of trade are achieved for the user, considering protocol fees, price slippage[7], etc. Moreover, the application layer may also include automated trading bots that seek and exploit arbitrage opportunities in DeFi markets. In a nutshell, the application and aggregation layers of the DeFi Stack may be considered as the front-end solutions while the settlement, asset and protocol layers are the back-end solutions.

3 DeFi Ecosystem

The primary features of DeFi being the disintermediation, composability and decentralised governance as well as non-custodial liquidity pools and smart contracts collectively provide for enhanced financial services to the crypto asset's holders. These consist of decentralised lending, trading, investment and insurance services.

3.1 Stablecoins

Stablecoins are essentially used as collateral[8] in DeFi protocols and thereby act as enablers of decentralised financial services. Due to the disintermediated and quasi-anonymous nature of DeFi, most DApps require user's collateral in order to function. Stablecoins[9] are typically pegged to fiat or the price of assets[10] in order to maintain their stable value, as compared to the rest of the crypto assets market. Also, these crypto assets allow holders of volatile crypto asset to retain their exposure by pledging their assets as a collateral in a smart contact in exchange for stablecoins that are accepted be a variety of DApps.

3.2 Trading

Trading in DeFi takes place through decentralised peer-to-peer crypto asset exchanges ('DEXs') such as Curve and Uniswap. The non-custodial nature of such platforms enables users to remain in full control of their assets

[6] Composability refers to the interoperability between different DeFi protocols.
[7] The 'probability that the deal terms will change over time' (IOSCO 2022, p. 16)
[8] This is similar to traditional deposits and other deposit-like instruments such as repurchase agreements.
[9] Stablecoins may be minted using either off-chain collateral that is held by the custodian or using on-chain collateral that is locked up in a smart contract.
[10] These mays be both crypto or real-world assets, or a combination of both.

throughout the interaction with the protocol. DEXs mitigate counterparty risk because prior to trade execution both counterparties to trade lock their crypto assets in the smart contract which then executes a simultaneous exchange of assets. On the other hand, centralised exchanges would require funds to be deposited with the exchange (or custodian) prior to trading. In consequence, DEXs eliminate the need for central counterparty clearing houses or escrow services.

Different implementations of DEXs exist on the blockchain, some are analogous to request-for-quote systems in traditional finance while others operate a decentralised order book. However, the most common type of DEXs that are currently implemented are Automated Market Makers ('AMM'). In simple terms these consist of smart contract powered liquidity pools that hold at least two (2) different crypto assets and allow users to exchange tokens by deposit one type of token in exchange for the other. The prices of the trading pair are set by means of a constant function[11] formula.

3.3 Lending

Lending protocols are one of the most widely used DApps in DeFi space as of today. The most popular current implementation of lending protocols such as Aave and Compound are similar in nature to the liquidity pool model outlined in Section 3.2, above. Lenders supply liquidity to borrowers of crypto assets by depositing tokens in the credit pools. These are essentially smart contracts that monitor the ratio of assets in the liquidity pool and automatically adjust the collateral requirements and interest rates[12] on ongoing bases for the borrowed assets. In is also worth noting that, unlike in TradFi where borrower's creditworthiness is assessed as a control for credit risk, in decentralises lending (where borrowers are quasi-anonymous) collateralised lending is prevalent. By means of collateral deposits, lending DApps account for credit risk as well as allow borrowers to gain access to new crypto assets whilst retaining their exposure to their original tokens, until the debt is repaid.

Finally, because of specific features of the blockchain technology an unprecedented form of lending has emerged in the DeFi markets, known as the 'Flash Loans'. Essentially, this DeFi solution allows borrowers to secure uncollateralised and virtually unlimited[13] loans instantaneously. However, flash loans are conditional to the loan being received, used and repaid within a single block of transactions that are recoded on the blockcahin network. Should the borrower fail to return the borrowed funds then the entire scheme is invalidated by the network and the transaction is not recorded on the chain.

3.4 Asset Management

In TradFi investors use asset management services in order to rely on the expertise of the investment fund manager and gain exposure to markets that may be unattainable on individual basis. Moreover, the fund manager would be responsible for the management and rebalancing of the pooled funds in order to achieve the fund's investment objectives whilst relying on a third-party custodians to hold clients' assets. Alternatively, in blockchain based asset management and advisory protocols can take various forms. In their purest form the reliance is placed on the software algorithms to ensure that the investment objectives and parameters met. In practice the protocol would follow an automated investment strategy by rebalancing the portfolio accordingly. More complex forms of DeFi asset management would include yield-farming aggregators that provide a type of asset management which has similar characteristics to robo-advisory service. Some examples of asset management protocols include Set and Convex

[11] An example of constant function may be x * y = k where x & y are the reserves of the 2 types of tokens while k is a constant.
[12] Interest rates are automatically adjusted based on levels of token liquidity; when liquidity is abundant, the interest rates will be low and vice versa.
[13] Borrower may choose to borrow an entire supply of token in the credit pool using a flash loan.

3.5 Derivatives

Derivative protocols such as Ribbon Finance and Synthetix are economically similar to the TradFi (options, swaps etc.) essentially, they allow participants to issue synthetic crypto assets that derive their value from the underlying reference asset ('asset-based') or the outcome of an event ('event-based'). Similarly, to the credit pools described above, issuers of synthetic tokens are required to deposit collateral into the smart contract in order for synthetic tokens to be created. The price of the underlying assets is usually tracked by means of a price 'oracles'[14] that provide up to date off-chain information/data to the blockchain. Other form of synthetic tokens also known as 'wrapped' or 'bridged' tokens are crypto assets that serve as a representation of original token on different blockchains by means of a 'bridge'[15].

3.6 Insurance

DeFi insurance services such as Nexus Mutual and InsureAce primarily revolve around risks that are specific to the decentralised blockchain environment. Such risks primarily emanate from DApp hacks, protocol failures and decentralised governance. Just like the rest of the major DeFi activities insurance are collateralised by the insurance policy holders and in the event where insurance claim is triggered the policy holder is reimburse from the pooled funds. The amount of pay-out is determined through a vote by claim assessors who would most likely be other policy holders of the same insurance pool.

4 Benefits and Risks

When evaluating new technology, benefits over the existing system are often revolutionary. In this regard, it goes without saying that DeFi restructures traditional finance services through its departure from centralised entities. However, such swift advancements present vulnerabilities in the emerging system, both technological and legal. Thus, it is important for one to have a clear understanding and assessment of the risks before deploying their capital in DeFi ecosystem. Building on the qualities of its underlying technologies, below is a non-exhaustive list of benefits and risk presented by decentralised financial service.

BENEFITS

Decentralisation – The disintermediation brought by decentralised applications allows for frictionless and faster execution for users whilst also cutting intermediary and other administration costs.

Transparency – Interaction with DeFi applications, although visible for everyone pseudonymously, provides a base for efficient auditing of protocol solvency as well as transaction transparency of the DApp's participants.

Efficiency – DeFi transactions do not rely on central counterparties, but can execute guaranteed transactions atomically which improve speed, costs and eliminate human intervention.

Accessibility – Given that some SMEs may currently have limited liquidity and credit opportunities, these SMEs may utilise decentralised applications for payments and other activities like lending, promoting financial inclusivity.

[14] Oracles supply real-world off-chain data to the blockchain protocols, such as price feeds from the centralised crypto assets exchanges or weather conditions. They form part of the application layer and are vital to the functioning of DeFi ecosystem.
[15] A 'bridge' is essentially a smart contract that links separate blockchains.

RISKS

Illicit Financing – DeFi protocols may not have proper KYC and no AML requirements and checks that mitigate terrorist financing or other illegal activities from taking place.

Rug pulls – The promotion of fraudulent schemes in DeFi, resulting in a loss of user funds or private key theft, often tied to anonymous developers.

Excessive leverage – Certain decentralised applications may offer excessive amounts of leverage at very close liquidation levels and expose users to mass liquidation events, leading to the loss of the user's trading funds and collateral.

Protocol bugs and exploits – Certain flaws in a smart contract's code may be exploited resulting in the loss of liquidity pool funds through repeated flash loan exploits or the draining of the entire liquidity pool in one transaction. Flaws in smart contracts may also lead to the lock of funds making users' crypto-assets permanently inaccessible, with no legal repercussions.

Impermanent loss – Impermanent loss occurs when the price of the deposited asset in a liquidity pool changes by the time a user is to withdraw it. This results in a loss of value of the investors' deposited asset compared to the same asset had it been held outside the liquidity pool.

Although, new systems like DeFi pose certain new risks, attributed to a maturing sector, it is important to note that other risks will always exist, regardless of the system used. Illicit financing and fraud are both risks which cannot only be attributed to DeFi but also traditional finance and thus one must not stifle innovation in finance because of certain risks but aim to harmonise regulation and innovation to help mitigate certain risks.

In conclusion, DeFi, and its wide variety of DApps, has continued to improve upon the capabilities of traditional finance, by enabling fast and frictionless interaction among users, and has continued to forge a path forward into a new age of disintermediation and financial inclusion.

Supplementary Reads…

International Organisation of Securities Commissions (IOSCO) (2022), OR01/2022 OICV-IOSCO Decentralised Finance Report. Available online.

Organisation for Economic Co-operation and Development (OECD) (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications. Available online.

European Financial Stability and Integration Review 2022. (European Commission) (2022). Available online.

Financial Stability Board (FSB) (2019), Decentralised Financial Technologies Report on Financial Stability, Regulatory and Governance Implications Available online.

Check our other **FinSights** and should you have any queries or wish to discuss your ideas, even within the context of our **MFSA Fintech Regulatory Sandbox**, contact us at **fintech@mfsa.mt**.