

Decentralised finance (De-Fi): Is this the future of finance?



AUGUST 2021

BLOCKCHAIN AND CRYPTOASSET (K) LTD.

Authored by: Patrick Kiragu Mwangi BA, BSc., MA



“The aim is to democratise finance by replacing legacy, centralised institutions with peer-to-peer relationships that provide the full spectrum of financial services – from everyday banking services, loans and insurance to complicated financial contracts including derivatives-trading and asset-trading.”

Traditional finance

Finance is a broad term that describes activities associated with banking, leverage or debt, credit, capital markets, money and investments. It also encompasses the oversight, creation and study of money, banking, credit, investments, assets, and liabilities that make up financial systems.

Today, almost every aspect of banking, lending and trading is managed by centralised systems operated by governing bodies and gatekeepers. Regular consumers of financial activity also have to deal with a raft of financial middlemen if they need to access anything from loans and mortgages to trading stocks and bonds. As a result, there are few paths for consumers to access capital and financial services directly. They cannot bypass these middlemen who earn a percentage from every financial and banking transaction as fee or profit.

This centralised global structure means that financial services are not readily available to many especially those who live in remote parts of the world. Further, financial decision-making remains undemocratised meaning that a handful of influential individuals and entities play a disproportional role in the running of the global financial system.

Decentralised Finance

Decentralised Finance, or 'De-Fi' in short, is an umbrella term encompassing a financial system that functions without any intermediaries such as banks, insurance companies or clearinghouses and that is operated just by the power of 'smart contracts'. It strives to fulfill the same functions as traditional finance but in a completely permissionless, global and transparent way. The aim is to democratise finance by replacing legacy, centralised institutions with peer-to-peer relationships that provide a full spectrum of financial services- from everyday banking services, loans, and insurance to complicated contractual relationships like derivatives-trading and asset-trading. It challenges the existing centralised financial system, disempowering middlemen and gatekeepers and passing on this power to everyday people via peer-to-peer exchanges.

In essence De-fi differs from traditional finance in the following ways:

- At their core, De-Fi operations are not managed by an institution and its employees. Instead, the rules are written in code (or 'smart contract'). Once the 'smart contract' is deployed to the blockchain, De-Fi decentralised applications (dApps) can run themselves with little to no human intervention (although in practice developers often do maintain the dApps with upgrades or bug-fixes).
- The code is transparent on the blockchain for anyone to audit. This builds a different kind of trust with users because anyone has the opportunity to understand the contract's functionality or find bugs. All transaction activity is also public for anyone to view. While this may raise privacy questions, transactions are pseudonymous by default, i.e. not tied directly to the users' real-life identities.
- DApps are designed to be global from the outset. Wherever in the world one is, they have access to the same De-Fi services and networks as everyone else with access. Though local regulations may apply, most De-Fi apps are available to anyone with an internet connection.
- 'Permissionless' to create and participate in. Anyone can create De-Fi apps and anyone can use them. Unlike finance today, there are no gatekeepers or accounts with lengthy forms. Users interact directly with the 'smart contract' from their crypto wallets.

- **Interoperable.** New De-Fi applications can be developed by combining other De-Fi products in the same manner as Lego pieces. For example, stablecoins, decentralised exchanges and prediction markets can be combined to form entirely new products. As such, De-Fi applications on public blockchains will potentially revolutionise financial markets as well as create entirely new products and services.
- **Full control.** Users maintain full control over their assets and interact with this ecosystem through peer-to-peer dApps.

The value proposition of De-Fi, therefore, lies in leveraging technology to reduce or eliminate the costs, time and risks associated with using traditional intermediaries and to expand access to innovative and traditional financial instruments to more market participants.

The vast majority of De-Fi protocols operate on the Ethereum blockchain, the world’s leading 'smart contract' platform. There are currently over 200 De-Fi applications on Ethereum, ranging from decentralised exchanges and lending protocols to trustless derivatives trading platforms and yield-generating liquidity pools. To date, the De-Fi market has grown into a multi-billion dollar industry with over \$56 billion locked up¹ in De-Fi protocols as of April 2021.

TOTAL VALUE LOCKED IN DE-FI (MAY ‘20 - APRIL ‘21)



Source: DeFi Pulse

¹ Industry observers measure traction with a unique new metric – ‘ETH locked in De-Fi’.

As the De-Fi market continues to grow, new protocols are being created to address new market needs as well as build new and innovative models for financial contracts. De-Fi is now, also, one of the fastest growing sectors within the crypto space.

Currently, the largest use-cases in De-Fi are:

I. *Monetary Banking Services*



As De-Fi applications are by definition financial applications, monetary banking services become an obvious use-case for them. De-Fi's financial architecture supports blockchain-based currencies, which must maintain a stable value at least within the settlement period (i.e., the time required for generating decentralised consensus on transaction records), in order for them to act as a viable means of payment. However, most of these cryptocurrencies² are highly volatile as they are platform-specific currencies whose values are unbacked and fluctuate along the supply and demand dynamics native to the hosting platforms. This substantial volatility exhibited by them serves to limit their use as a viable means of payment.

With the advent of stablecoins³ and their issuance as part of a decentralised monetary system, De-fi may have come up with a solution to the volatility problem. Stablecoins provide the same value to cryptocurrency investors, traders and exchanges that fiat money provides to the participants in the traditional financial markets, namely stability. While fiat currencies, like USD or EUR, are backed by the confidence the market has in the issuing governments, stablecoins can be backed by actual assets. By

² The terms 'cryptocurrency' and 'cryptoasset' are used interchangeably in this report to mean the same thing.

³ Stablecoins are a type of cryptoasset that are typically pegged to a real-world asset such as the US dollar or gold, therefore, bringing some degree of price stability to the market, but that can also be equally transferred digitally with relative ease.

keeping their value pegged in this way, they offer a level of stability in the volatile crypto market.

Further, while traditional investors will allocate portions of their portfolios to cash, treasury bonds or money-market funds when volatility is on the rise, cryptocurrency investors move to stablecoins during such times. Stablecoins then become the link between decentralised finance and the real economy since, designed to have a stable exchange rate with respect to the reference fiat currencies, they have the potential to mediate transactions of goods, services, and real assets. Stablecoins are also important for the cryptocurrency community. Traders' activities heavily involve rebalancing between stablecoins and more volatile cryptocurrencies.

Ultimately, the aim of De-Fi here, is to build a monetary and banking system based on blockchain and stablecoins through the issuance of the latter. In this, the issuance of stablecoins will play the role of money-creation in some form of shadow-banking through the unregulated creation of safe assets to meet users' transactional demand and beyond.

There are generally three types of stablecoins. Fiat-collateralised stablecoins like USDT, USDC and BUSD store their value in fiat currencies and are typically redeemable at a 1:1 ratio with the pegged fiat currency. However, this type of stablecoins require trust in a centralised entity and are, therefore, vulnerable to loss of peg and destabilisation from external geopolitical factors. Crypto-collateralised stablecoins like DAI are backed by other cryptocurrencies such as ETH, USDC and BAT and rely on trustless issuance. They maintain their 1:1 peg against these other cryptocurrencies through algorithmic methods including over-collateralisation and incentives. This trustless issuance makes this type of coin wholly transparent and the reserve auditable. Non-collateralised stablecoins like AMPL use an algorithm whereby the system supplies more tokens with increased demand while the price of each token is lowered and vice versa to maintain a stable peg.

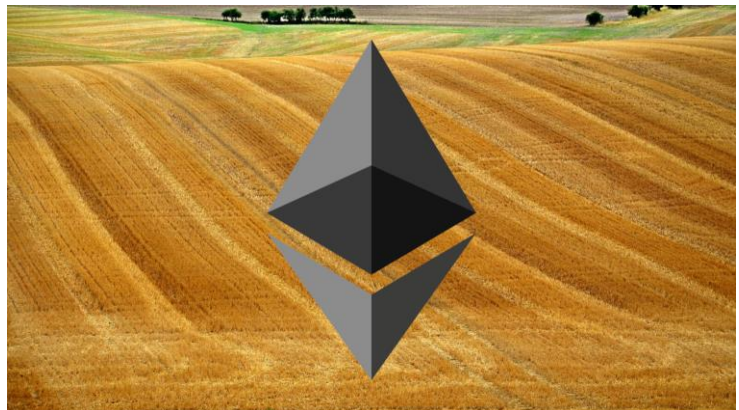
The stablecoin monetary base reached over \$65 billion in Q1 2021 and continues to rise at an accelerating pace having reached a whopping \$1 trillion in transaction volume during the same period.

II. *Peer-to-peer (pooled) lending & borrowing services*

De-Fi peer-to-peer lending and borrowing, like with traditional finance, entails the act of one-party providing assets (here digital in nature) to another in exchange for a steady income stream paid in the form of interest. As such De-Fi enables users become lenders or borrowers in a completely decentralised fashion such that an individual has complete control over their funds at all times. This is made possible via the use of 'smart contracts' that operate on open blockchain solutions such as Ethereum.

De-Fi credit protocols have now become some of the most popular types of applications within the wider De-Fi ecosystem. Since they are built on public blockchains they minimise the amount of trust required and carry with them the assurance of cryptographic verification methods. This reduces counterparty risk and makes borrowing and lending cheaper, faster and readily available to a wider public. Other advantages over the traditional credit system include instant transaction settlement, the ability to collateralise digital assets, nil credit checks and a potential standardisation of the credit system in the future. Right now, it can be near impossible for the unbanked to borrow money, often because they lack credit records and history with a banking institution. The De-Fi credit platforms connect borrowers and lenders directly.

Arguably the most talked-about trend in today's De-Fi market, and a component of peer-to-peer lending and borrowing, is 'yield farming'. This involves placing cryptoassets into De-Fi protocols to generate the highest possible returns.



This can take various forms with the most common being depositing funds in high-yield lending protocols like Compound and Dharma. Investors looking for more yield than traditional fixed-interest investments — such as savings accounts, money-market funds or bonds — can, therefore, digitise their funds within these protocols to earn

superior yields. Lending rates on protocols like Compound, DYdX and Aave range from 0.15% to 11.82% Annual Percentage Yield (APY)⁴.

A play on ‘yield-farming’ is ‘liquidity mining’ which involves providing liquidity to De-Fi protocols such as decentralised exchanges in return for newly minted protocol tokens. De-Fi protocols Balancer and Compound, for example, reward liquidity providers with protocol-native tokens for participating on their platforms. As these tokens can be traded on the secondary market, an incentive structure is created where investors can earn substantial returns in the form of protocol tokens for contributing as much capital to a protocol as possible and trading these onwards.

‘Yield aggregators’ are an additional innovation in the space and seek to find the best ‘yield-farming’ opportunities across Ethereum’s entire De-Fi ecosystem and then automatically moving the user’s investment to the vehicles with the best returns. The result is much more diversification for investors paired with significantly higher returns. Yearn Finance, one of the leading ‘yield aggregation’ protocols, uses automation to maximise profits from yield-farming for users.

The following are some of the leading peer-to-peer lending and borrowing De-Fi protocols.

- Compound

Compound is an autonomous blockchain-based borrowing and lending dApp, enabling users to lend crypto out and earn interest; or deposit crypto in the Compound protocol as collateral and borrow against it.

- Maker

Maker is a unique De-Fi crypto-lending platform that allows borrowing only DAI tokens. Users can use Maker to open a vault, lock in collateral like ETH or BAT and generate DAI as a debt against that collateral.

⁴ Annual percentage yield (APY) is the effective rate of return on an investment for one year taking into account the effect of compound interest.

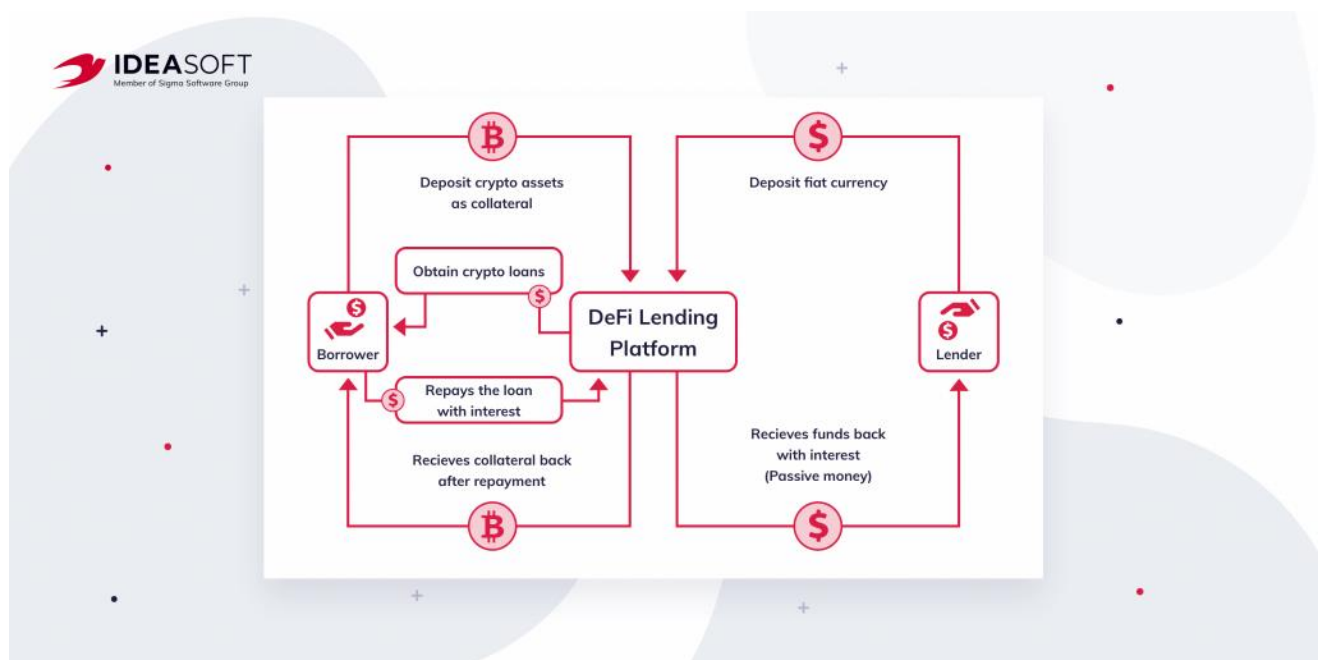
- Aave

With Aave, users can use a cryptocurrency like Bitcoin as collateral and receive a stablecoin loan or flash loan at attractive interest rates.

- Dharma

Dharma is a savings protocol and money-management app that enables users manage their Ethereum tokens and invest them in De-Fi protocols to earn investment income.

How do De-Fi lending platforms help the financial services sector?



Source: IdeaSoft

III. *Tokenisation*

As is evident from the foregoing, almost all financial products and services offered today by traditional firms can be provided through De-Fi and tokenisation; though not all these products and services have mature markets or are yet fully developed at this point. Tokenisation refers to the issuance of tokens on blockchain-based protocols to represent practically any real-world asset. This way assets like art, property, commodities, stocks, etc can be owned and traded on blockchain. Tokenisation is, therefore, not limited to cryptocurrencies only but, rather, can be used to include a

whole range of real-world assets, thereby, presenting endless opportunities for innovation. It is yet an additional tool to democratising access to markets.

In essence, De-Fi infrastructure now offers the potential for tokenised assets to participate in new full-fledged money markets. Within these newly-emerging secondary markets, a borrower could put their tokenised stake in a business down as collateral and take out a loan. The token is fitted with information that is important to both the issuing party and the investor who buys the token. This creates an automatic and efficient secondary market which doesn't require needless third-party verification nor intermediaries to enforce trust as is current with the existing legacy system. In the De-Fi system, trust is outsourced to the computer programs and continuously executed.

The tokens can also be differentiated based on geography, capital, risk-profile, sectors, industries and regulatory-authority, for instance, and are not controlled by any one party. Each point of differentiation can be monitored through data oracles which retrieve and update the information on a real-time basis. These oracles can be wrapped in a 'smart contract', which is triggered automatically, and put on a blockchain so that it remains open and distributed.

De-Fi and tokenised instruments can be employed by companies at all stages of growth- from start-ups to established, billion-dollar behemoths and from private corporations to publicly-traded companies with multiple share classes. As such the benefits of tokenisation for companies can be summarised as follows:

- ★ *Increased liquidity*- the ability to tokenise illiquid, private and other types of assets allows their trading on secondary markets of the issuer's choice. Increased access generates a liquidity premium and can cause greater value to be derived from the underlying assets
- ★ *Increased Speed*- with fewer human intermediaries and the utilisation of 'smart contracts', steps can be automated and/or eliminated thus speeding up transactions
- ★ *Lowered Cost*- with fewer human intermediaries and the use of automation via 'smart contracts', transaction costs can be reduced compared to traditional finance methods

- ★ *Risk mitigation*- although cybersecurity is never guaranteed and new threats always arise, tokenisation allows for greater exertion of operational risk control and visibility
- ★ *Transparency*- securitised tokens can hold the token-owner's legal duties and rights on the token itself. Furthermore, an unchangeable record of ownership is recorded on the token itself as well
- ★ *Access and innovation*- by reducing the number of intermediaries and enabling lower costs, new products can be developed since they are not as contingent upon volume as traditional financial services are. In addition, tokens can be fractionalised allowing for more investors to be able to afford them and, thereby, augmenting flexibility for both issuers and investors

A prime example of tokenisation is Wrapped BTC (WBTC). Wrapped BTC is an ERC20 token – backed 1:1 by bitcoin – that enables bitcoin-holders to use tokenised bitcoin in Ethereum-powered dApps and trade it on decentralised exchanges.

IV. *Decentralised Exchanges (DEXs)*

Although centralised exchanges (CEXs) currently dominate cryptocurrency trading activity, disintermediation as a core philosophy of the blockchain community has meant that decentralised exchanges (DEXs) have continued to gain popularity alongside the more established CEXs. DEXs are De-Fi platforms that facilitate peer-to-peer trading by relying on automated 'smart contracts' to execute trades without involving a trusted intermediary (the cryptocurrency exchange). This dynamic enables instantaneous trades often at lower cost than on CEXs. By cutting out crypto exchanges and similar-structured custodians, these platforms help eliminate single points of failure aligning them with what has made the blockchain technology so powerful in the first place.

In the absence of intermediaries, DEXs take on a non-custodial framework which means that the custody of cryptoassets remains with the investor themselves and they are responsible for

managing their own wallets and private keys, thereby, giving them full control of their assets.

However, this comes with the risk that the keys could get lost, stolen or destroyed. This dispensing with an intermediary has the added advantage that most DEXs have limited counterparty risk and there is not the requirement to have in place Know-Your-Customer (KYC) or Anti-Money-Laundering (AML) protocols.

DEX volumes had reached a total volume of over \$217 billion as at Q4 2020.

DEXs that are currently available include:

- Uniswap

Uniswap is a DEX that runs entirely on 'smart contracts', letting the user trade popular tokens directly from their wallet. The protocol uses an innovative mechanism known as Automated Market Making (AMM) to automatically settle trades near the market price.

- Balancer

Balancer is an AMM protocol that rewards 'liquidity pool' participants with its governance token, BAL, on top of pool fees. The more protocol participants contribute to a pool, the more they will earn in governance tokens.

- Binance DEX

Binance DEX operates through a web-based application programming interface (API) that uses a similar user interface to Binance.com. The exchange offers the same functionality as a typical DEX, but also integrates TradingView charts with technical indicators.

- Sushiswap

SushiSwap emulates Uniswap except that it started by offering liquidity providers a token known as SUSHI (which Uniswap later also offered with its UNI token).

- Kyber

The Kyber protocol operates as a stack of 'smart contracts' that run on any blockchain, not just Ethereum. It utilises 'liquidity pools' to facilitate peer-to-peer swaps.

- Bancor

One of the earliest DEXs, Bancor allows users to borrow assets against their staked liquidity, essentially combining the benefits of 'yield-farming' and lending into a seamless user experience.

- Gnosis

The Gnosis protocol pools liquidity through a unique mechanism called 'ring trades' which function as order settlements that share liquidity across all orders, not just a single trading pair.

- Curve Finance

Similar to Uniswap, Curve utilises a liquidity pool and specifically caters to stablecoin trading, allowing users to trade between them via an algorithm that optimises trading pairs.

- Loopring

Since Ethereum's gas fees are a major obstacle for smaller traders, Loopring launched a DEX on layer 2, offering users cheaper transaction fees without sacrificing the security of Ethereum.

- DYdx

The DYdX protocol allows users to access derivative products in a decentralised environment and also supports peer-to-peer borrowing, which means investors can earn passive income while their cryptoassets are held on the exchange.

The main benefits of DEXs include:

- ★ trustless, which means that users' funds and personal data are safe
- ★ security and privacy are well preserved
- ★ users control their own cryptoassets
- ★ DEXs represent a global marketplace

However, DEXs have certain limitations:

- ★ DEXs retain the same scalability problems as the underlying blockchain
- ★ most DEXs are not easily usable, struggle with liquidity and do not support fiat payments

V. *Derivatives*

Derivatives are one of the key elements of any mature financial system with their two main use-cases being as hedging instruments and as means of speculation. Within the DeFi space, hedging allows for the managing of financial risk enabling crypto companies hedge their exposure to different crypto-based technologies (protocols) and run more predictable businesses. Investors are also able to hedge against risk in the crypto space using derivatives. Yield-farmers, for example, can use derivatives to offset a potential loss that can occur if the price of one of the tokens used for 'yield-farming' loses its value in relation to another token.

Aside from hedging as a use-case for derivatives, speculation within the De-Fi space has helped bring additional trading volume to the market because derivatives, by their very nature, offer easy exposure to particular assets that may be hard to otherwise access. They also provide easy access to leverage – a trader can purchase a call or a put option by providing only enough funds to cover the option premium but gain exposure to a significant amount of the underlying cryptoasset. Speculators are, therefore, important market participants as they provide liquidity to the market and allow people, who actually need to buy a particular derivative to hedge their risk, to easily enter and exit the crypto market.

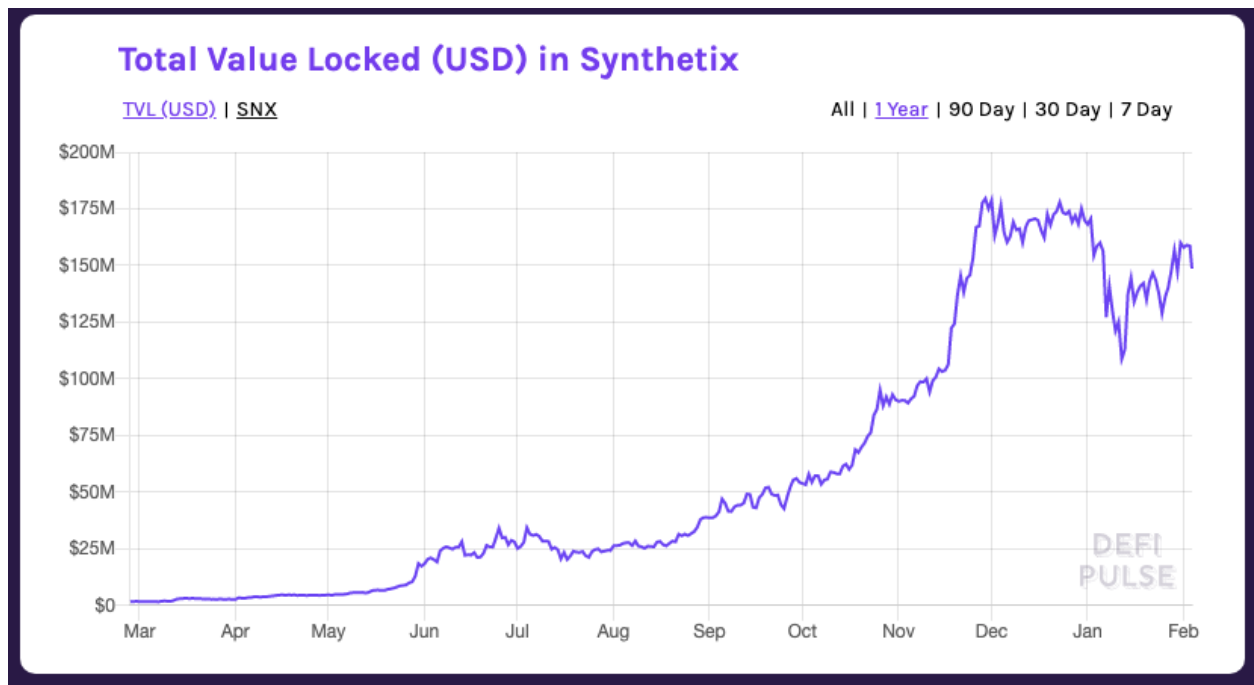
Decentralised derivatives are slightly different from traditional derivatives in that they don't require a broker. Instead, the terms of the contract can be programmed into 'smart contracts', thereby eliminating the need for a third-party. Settlement automatically takes place on-chain when the terms of the contract are fulfilled. The flexibility of decentralised derivatives is, therefore, vast enabling users to create instruments on virtually any underlying asset. Decentralised derivatives account for around 18% of the total value locked in De-Fi and is the second most popular category of De-Fi dApp after lending.

Every growing market naturally develops its own derivatives market that can end up being an order of magnitude bigger than its underlying market. This is one other reason a lot of people in the De-Fi space are extremely bullish on the potential of decentralised derivatives that, in contrast to those in traditional finance, can be created by anyone in a completely open and permissionless way.

Some of the most important derivatives protocols in De-Fi include:

- Synthetix

Synthetix allows for creating synthetic assets that track the prices of their underlying real-world assets. The protocol currently supports synthetic fiat currencies, cryptocurrencies, commodities and indices that can be traded on trading platforms such as Kwenta, DHedge or Paraswap. Currently, Synthetix is the most dominant decentralised derivatives application accounting for 98% of the value locked in De-Fi derivatives.



Source: De-Fi Pulse (2020-21)

- UMA

UMA is another protocol that enables the creation of synthetic assets. It is a decentralised platform enabling the creation of self-enforcing financial contracts. Any two parties can create a customized financial contract, specifying the terms including margin requirements and termination conditions.

- Hegic

Hegic is a relatively new De-Fi project that allows for trading options in a non-custodial and permissionless way. Users can buy put or call options on ETH and WBTC. They can also become liquidity providers and sell ETH call and put options.

- Oryn

Oryn also allows for trading options. It launched in early 2020 and started by offering ETH downside and upside protection which allowed users to hedge against ETH price movements, flash crashes and volatility. They have recently launched a V2 of the protocol that offers European⁵, cash-settled options that auto-exercise upon expiry. In contrast to Oryn, Hegic uses American-style options.

- Perpetual

Perpetual allows for trading perpetual contracts. A perpetual contract is a derivative financial contract with no expiration or settlement date; hence it can be held and traded for an indefinite length of time.

- BarnBridge

BarnBridge is a risk-tokenising protocol that allows for hedging yield sensitivity and price volatility. This is achieved by accessing debt pools of other De-Fi protocols and transforming single pools into multiple assets with different risk/return characteristics.

- Vega

Vega is a decentralised protocol for trading margined financial products. Participants are able to create their own products, such as options and futures, using Vega's 'smart product' language.

- CloseCross

CloseCross is developing a decentralised, multi-party derivatives trading platform. It aims to make it simple for anyone to enter the derivatives market by simply choosing an underlying asset, a prediction and a time period.

⁵ European options can only be exercised at the time of expiration whereas American options can be exercised at any time up to the expiration date.

VI. *Prediction Markets (PMs)*

A prediction market (PM) is a place to buy and sell predictions or bets and this relies on the collective wisdom of the crowd for a correct outcome. PMs have been used as tools for generating accurate forecasting information in order to hedge against real-world risks and for making trading gains. Their most common and traditional use has been in forecasting sport, political or economic events and examples of these markets include PredictWise, The Iowa Electronic Markets and BetFair.

For their part, blockchain-powered PMs attempt to change the world, from politics to science, by creating digital democracies with a new age of financial tools. They utilise the technology of 'smart contracts' for bets on various issues. Examples include Augur, Bitcoin Hivemind, Amoveo, Gnosis, Polymarket and Cindicator.

Both these markets (traditional and blockchain-based) are literally used to answer questions or predict outcomes. Those who believe they have superior knowledge to the market can bet and potentially earn a reward for this. The market price adjusts in response to what the crowd thinks the probability of the event is over time. The possibility of making a profit lies in deviating from or disagreeing with the consensus and therefore experts, actuaries and companies with advanced prediction capabilities are incentivised to participate to the disadvantage of ill-informed opinions. The possibility of making a loss motivates participants to exercise more caution and become more objective with their opinions and decision-making.

Before Augur⁶ came along, prediction markets were only open to centralised parties like bookmakers or brokers, making them susceptible to anti-gambling regulations. Now anyone can open up a prediction market based on any real-world outcome. The highest bets, as a rule, are made by the most competent bettors since they count on winning more than the others. This is where blockchain-based oracles come into play. They inform the blockchain network whether the prediction was right or wrong. After the

⁶ Augur is a decentralised blockchain-based PM protocol that allows users to vote on the outcome of events by attaching a value to the vote. With Augur users can vote on the outcome of events, except that they have to place bets by attaching a value to their vote. It can be considered a kind of fusion between betting and derivatives and acts as a decentralised oracle and platform for prediction markets.

information is transferred, the bets of those who lost are automatically transferred to the winning party.

VII. *Insurance*

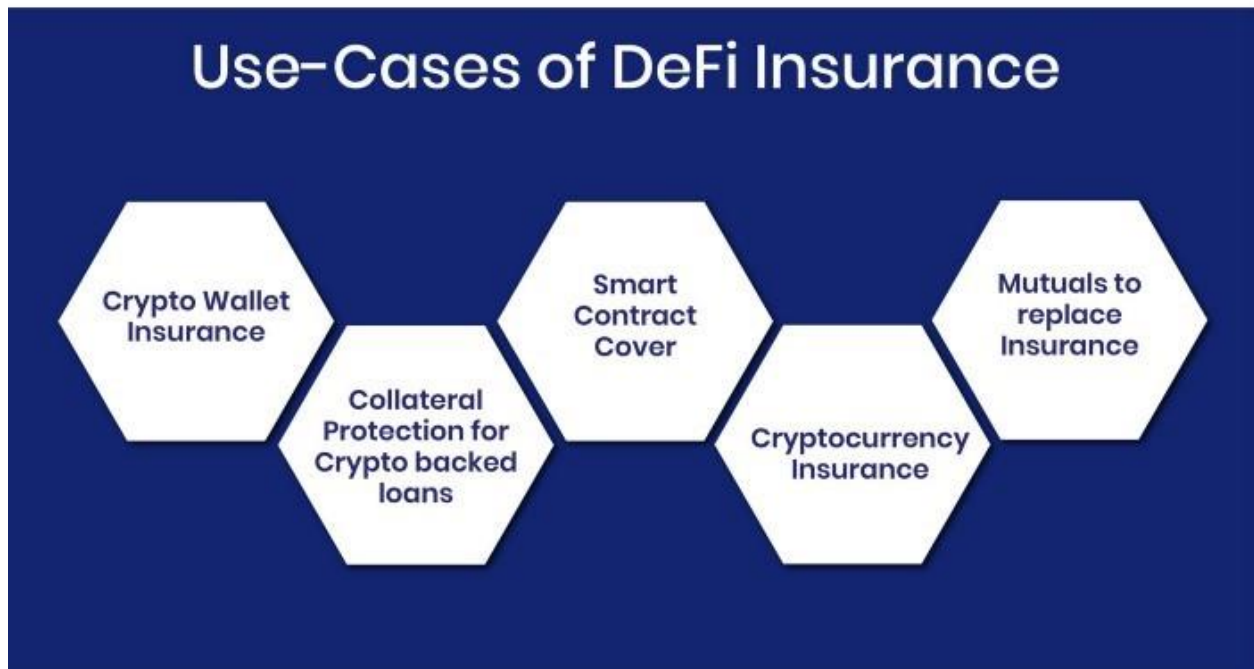
The De-Fi market as a form of new age finance can be a fairly risky space. The nature of 'smart contracts' and decentralised protocols makes them subject to exploits and hacks, occasionally leading to significant losses for affected users. These include flash loan hacks that exploit weaknesses or 'loopholes' in the 'smart contracts' that govern protocols, allowing canny actors to drain millions of dollars from their liquidity pools. To protect against these risks and threats, it has become imperative that there exist mechanisms that protect users and participants against them. Decentralised Insurance is one such innovation that has emerged as a protective gear for the De-Fi sector leveraging blockchain technology to cover risks and protect cryptoassets.

Much like traditional insurance, it aims to protect users from losses in return for a specific premium based on the size of their holding and which platform they are holding it with. While a traditional insurance policy might be issued and underwritten by a multinational insurer, a De-Fi insurance policy relies instead on its community of users to dictate premiums and orchestrate payouts.

The main actors of a De-Fi insurance protocol are, therefore, the underwriters that provide capital to the insurance pools for each individual protocol covered and who take a share of premiums (also known as staking); the claims assessors and governance token-holders that vote on claims and changes to the protocol; and claimants or those that buy the insurance premiums. Depending on the protocol, underwriting (or staking) can be a fairly lucrative pursuit thanks to the regular income stream that is available from premiums, while rewards in the form of the native governance tokens also boost the haul considerably. As one might expect, the riskier the protocol the higher the premium paid⁷.

⁷ On Nexus, for example, it costs 0.1281 Ether (ETH) to insure 10 ETH on the Curve Finance protocol for a period of 180 days, while the same level of cover for the same holding on Acropolis Delphi comes with a 2.18 ETH price-tag (an APY of around 48%).

In essence, De-Fi Insurance products offer complete protection of De-Fi deposits, hedge against crypto volatility risk and flash crashes as well as provide security against the risk of theft and attack on crypto wallets. They also make the entire process of submitting, claiming and processing any payouts extremely safe, reliable and transparent.



Source: Blockchain Simplified

Over the last couple of years, there have been innumerable cases of ‘smart-contract’ hacking, cyber-attacks on exchange platforms, etc that have led to a huge loss of investor funds. Decentralised Insurance has a role to play in mitigating against these risks and offers the following:

➤ **Crypto Wallet Insurance**

Companies like Etherisc have developed solutions to cover the risk of theft of crypto wallets in case of attacks. Etherisc provides crypto wallet insurance covering large investment sums.

➤ **Collateral Protection for Crypto-backed loans**

In the case of crypto loans, if the collateral provided by the borrower is destroyed or stolen, then the loan is paid off by the insurance policy. Etherisc, along with companies

like Sweetbridge, Celsius, Nexo, Libra Credit and a few others have established a consortium that safeguards and secures collateralised crypto-backed loans.

➤ 'Smart contract' Cover

'Smart contract' cover insures against loss if the designated 'smart contract' address is hacked into leading to a loss of funds from an investor account or if funds are moved to another address which doesn't belong to the original investor. It also covers loss where the funds are permanently lost and cannot be recovered anymore. Nexus Mutual is one company that offers 'smart contract' cover.

Apart from Nexus Mutual and Etherisc, other De-Fi insurance protocols include CDx that offers covers for loss of funds that happen due to exchange hacks, Union Finance which has proposed a multi-token model and claims to be able to cover users beyond just 'smart contract' failure as well as Oryn and VouchForMe.

Risks and challenges



- Scalability

Even where De-Fi applications manage to attract millions of users to their platforms, the public blockchains they rely on may lack the capacity to meet such demand. Scalability concerns have also been a long-running thorn in the side of Ethereum especially since the

result is very high transaction costs – known as 'gas' fees – and long transaction-processing times. For De-Fi users this means absolute returns are diminished as they move in and out of De-Fi protocols.

- Regulatory fears and uncertainty

Even though stablecoins bring some level of price stability to the crypto market, lawmakers are concerned that such cryptocurrencies and others like Facebook's Libra (now renamed Diem) could undermine the U.S. dollar and throw the global economy

into disarray. Banks, for their part, fear that stablecoins could create a ‘shadow banking’ system to replace them in time.

- Lack of cohesion or consensus

A big drawback in achieving consensus between the different DeFi organisations is that these are working independently of one another thereby creating a fragmented market; and to compound the problem, there are countless governments with conflicting attitudes toward crypto and blockchain in general. Some countries have banned digital currencies in their entirety while others have continued to work closely with innovative companies in the space.

- Spectre of a market meltdown

Despite the stability within the crypto space brought about by stablecoins, there exist no clear legal and regulatory frameworks. Unlike depository institutions, a stablecoin issuer does not have any obligation to maintain redemption at par. Given that crypto reserves are often invested in risky assets, there is valid concern that a major stablecoin ‘breaks the buck’ thereby triggering financial turmoil.

- Conflict of interests

Stablecoins are issued by private entities who promise to maintain price stability by holding collateral assets against which stablecoin holdings can be redeemed. However, as these issuers maximise their own payoffs rather than the total welfare, conflicts of interests between the issuers and stablecoin-users naturally arise, making it imperative to enact welfare-enhancing regulations.

- Lack of investor protection

De-Fi has continued to thrive despite an absence of rules and regulations. However, this means that users and investors have little recourse should transactions go wrong or should particular platforms collapse.

- The requirement for collateral

Nearly all De-Fi lending transactions require collateral equal to at least 100% of the value of the loan, if not more. These requirements vastly restrict who is eligible for many types of De-Fi loans, defeating the very purpose of De-Fi.

- Market volatility

De-Fi protocols face the constant threat of borrow APYs rising dramatically within a short time-period. For example, during the De-Fi craze of 2020 where 'yield-farming' became a rage globally, borrow APYs on certain cryptocurrencies rose to 40% and over. This inadvertently meant that users who do not regularly track their interest rates daily had to repay way more, in interest rates, than they had anticipated.

- No pricing mechanism for tokenisation

Real-world assets that become tokenised must have a transparent source of pricing available on demand by any user of the De-Fi protocols. This requires building a price oracle that will gather and transfer information regarding the collateral. However, at present, there are neither publicly-available sources for pricing nor a mechanism to monitor the pricing in real-time. This contributes to great illiquidity in the space.

Last word!

Money and finance have been around in one form or the other since the dawn of human civilization. Blockchain and cryptocurrency are just the latest digital avatar and in time we should see every financial service that exists in today's fiat system being rebuilt and onboarded onto the blockchain ecosystem, namely as part of Decentralised Finance.

Decentralised Finance is focused on building financial services separate from the traditional financial and political system. This will allow for a more open financial system and could reduce censorship and financial exclusion across the globe. By decentralising key aspects of existing financial infrastructure- such as access, data and code these new and open crypto networks will help enhance inclusion and innovation and help reduce censorship and financial exclusion across the globe.

To date, De-Fi remains a playing field for experienced blockchain users and crypto investors who understand how to interact with 'smart contracts' and who manage multiple digital assets. The average retail investor is yet to enter the De-Fi market as the knowledge barriers are still quite high. However, if successful, De-Fi will take power from large centralised organisations and put it in the hands of the open-source community and the individual. It will enable anyone across the globe to access a

decentralised, global financial marketplace that provides all the services traditional financial institutions offer today.

De-Fi will provide for censorship resistance, worldwide participation and the elimination of trusted third parties within the financial ecosystem. However, establishing contacts between De-Fi platforms, unlocking new partnerships and engaging in conversations with decision-makers who can help this technology reach the masses, is nothing short of vital if crypto and blockchain are going to become a compelling alternative to the status quo.

Ultimately, it is not even a monetary question but a political one. For whatever is decided, it must have the 'consent of the people'. The future of money is too important a matter to be left entirely to central bankers; and, in a free-thinking democratic world, innovation should not be stifled by government and regulators in their bid to retain vested interests or cling on to old powers.

Time will tell.

APPENDIX

De-Fi cryptos by market cap. and sub-sector

Cryptoasset	Ticker	Mkt cap in \$billion (15/8/21)	Rank (15/8/21)	De-Fi sub-sector
Tether	<i>USDT</i>	63.4	5	Monetary Banking services
USD Coin	<i>USDC</i>	27.6	8	Monetary Banking services
Uniswap	<i>UNI</i>	17.7	10	DEX
Binance USD	<i>BUSD</i>	12.1	15	Monetary Banking services
Wrapped Bitcoin	<i>WBTC</i>	9.2	19	Tokenisation
Dai	<i>DAI</i>	6.0	26	Monetary Banking services
Aave	<i>AAVE</i>	5.3	28	P2P lending & borrowing
Maker	<i>MKR</i>	3.7	37	P2P lending & borrowing
Compound	<i>COMP</i>	2.6	50	P2P lending & borrowing
SushiSwap	<i>SUSHI</i>	1.6	68	DEX
Synthetix	<i>SNX</i>	1.5	71	Derivatives
yearn.finance	<i>YFI</i>	1.5	72	P2P lending & borrowing
Bancor	<i>BNT</i>	1.0	88	DEX

Curve DAO Token	<i>CRV</i>	0.9	97	DEX
UMA	<i>UMA</i>	0.8	105	Derivatives
Perpetual Protocol	<i>PERP</i>	0.6	110	Derivatives
Loopring	<i>LRC</i>	0.4	131	DEX
Gnosis	<i>GNO</i>	0.3	152	DEX Derivatives
Augur	<i>REP</i>	0.3	153	Prediction Markets
Balancer	<i>BAL</i>	0.2	189	DEX
DODO	<i>DODO</i>	0.2	193	DEX
Ampleforth	<i>AMPL</i>	0.1	301	Monetary Banking services
Hegic	<i>HEGIC</i>	0.1	350	Derivatives
BarnBridge	<i>BOND</i>	0.1	354	Derivatives
Nexus	<i>NXS</i>	0.05		Decentralised Insurance
Cindicator	<i>CND</i>	0.03	602	Prediction Markets
Etherisc DIP Token	<i>DIP</i>	0.03	605	Decentralised Insurance
Vega	<i>VEGA</i>	No data	2965	Derivatives

Kyber Network Crystal Legacy	KNCL	No data	5194	DEX
------------------------------------	------	------------	------	-----

Source: CoinMarketCap

DISCLAIMER

This is a promotional document and as such the views expressed do not constitute investment (or any other) advice nor a recommendation to buy, sell or trade cryptocurrency. Blockchain and CryptoAsset (K) Ltd. does not guarantee its accuracy, completeness or timeliness and as such the information is subject to change.

Past performance is not a guide to future performance.

Investing in cryptocurrencies is inherently risky and could lead to huge or even total monetary loss. Investors should, therefore, only invest money which they can afford to lose.

We accept no liability for any actions taken, or not taken, as a result of the information contained in this material. Reliance upon this information is, therefore, at the sole discretion of the reader.

Any research in this document has been obtained and may have been acted upon by Blockchain and CryptoAsset (K) Ltd. for its own purpose.

August 2021