AllStarsWomen
NFT Club & DAO

What is DeFi?

DeFi is an umbrella term for a vision of a financial system without any intermediaries, such as banks, insurance providers or clearinghouses,and is built on decentralised networks,using blockchain technology (mostly Ethereum at the moment,although it could be any other blockchain). Decentralised finance is based on open protocols and decentralised applications (dApps), which typically share these four key characteristics:

- custody: DeFi protocols claim thatusers of DeFi platforms typically have control of their own funds in their own crypto wallets relative to using centralised exchanges or platforms,unlike trading stocks where funds are typically beingheld at a custodian bank. However it seems to us that when crypto assets are placed into a smart contract

used by DeFi, it is akin to losing direct control,hence we don't think the "non-custodial" claim of DeFi protocols is 100% accurate. DeFi smart contracts can ensure that collateral can be escrowed without a custodian.

This means that the assets issued or managed by DeFi cannot be unilaterally

expropriated or altered by anyone other than the account owner,although changes in the protocols (via the relevant governance structure) may impact the economic rights of the digital assets holders.

- permissionless: there is no KYC / AML/ onboarding process,anyone can have access to financial services without being blocked,although there are permissioned models emerging, for example Aave Arc, which in our view introduces some centralisation elements to DeFi

- open source(transparent):anyone (with enough technical knowledge) can check the state of the system,verify protocols, for example to check collateralisation

- composable:new financial products and services can be created using the same

building blocks.For example,a stablecoin can be the collateral for a loan,and the loan can be subject to an insurance contract.

Smart contracts are applications stored on a blockchain and executed in parallel by a large set of validators,and they are key for providing financial services. Use cases span the different areas of finance, including paying, lending, borrowing, trading,and insuring.

Who uses DeFi?

Retail vs institutional

New applications of the cryptocurrency blockchains are being developed and launched every day. Many are part of Web 3.0, which aims to create systems and applications that are managed on blockchains instead of on centralised servers. These decentralised applications,known as dApps,are not just made for the financial world – art/collectibles (NFT marketplaces),gaming,and music contenthave been popular areas

of growth too. There are almost 4,000 apps listed on the State of Dapps website, with 40-50 being added every month since last August. Ethereum-based applications have on average over 50,000 daily users.

User growth and transactions rose steadily along with crypto prices for DeFiand DEX (decentralised exchange) applications. As we showed in Exhibit 19 total DeFinew user accounts grew at a comparable pace to the growth of Ether's price. The average ethereum traded per transaction grew rapidly last year, particularly as NFT trading became popular.For example,around 15% of Ethereum's gas fees (the transaction fee) on a daily basis are used on the largest NFT platform called OpenSea.

Which settlement layer? Battle of the Blockchains Ethereum remains the mostused blockchain for decentralised applications. That could change in the future as many other blockchains aim to take some of the market share.

As we have previously discussed (see High leverage meets regulation), the valuation of an individual cryptocurrency is difficult to assess today as the use cases are not fully developed.

Beyond the market speculating on which coin will suddenly gain a large following on social media or receive institutional investor interest, there are some fundamental aspects to the coins that can be considered. Somecryptocurrencies are the token that runs on a particular blockchain, with the name of the coin often being the same as the blockchain. So we could consider whether that blockchain may have an ultimate use

case to replace something (transactional) we are already doing another way in society. Over the past two years there has been an increase in activity on the Ethereum blockchain from cryptocurrency trading activity, interest in NFTs and growth of transactions via decentralised finance lending and exchanges. More users on Ethereum led to higher transaction costs last year ("gas fees") and congested the network.

Currently there is a limit on the number of transactions that can occur per second on Ethereum but that be eased through scaling strategies where parts of transactions are checked away from the main blockchain (called 'rollups').

Competitors came along in the market, offering lower transaction costs

and faster transaction times. Exhibit 14 lists a range of blockchains and

their maximum number of transactions per second,according to the

creators. Cryptocurrencies thathave appreciated in value recently and

outperformed others have done so on the assumption that their related blockchains can handle much more transaction volume than Ethereum and so will take market share. This metric is the

"fundamentals" of the coin that could be used for valuation.

For example Ethereum handles 5x the number of transactions relative

to Bitcoin but Polygon and Solana can handle 65,000 transactions per

second relative to around 15 for Ethereum currently. The large difference has meant more applications (dApps)have moved to work

on these other blockchains, providing the use cases.

We expect the coming months and years to see different blockchains

picking up market share and becoming popular. We cannot say today

that one of the known blockchains will "win" in the end as the market is

still young and use cases are being discovered. Each of theseblockchains also has a different developer community, some of which may be trusted

more by the markets than others. The battle of the blockchains will continue.

Exhibit 13shows that Ethereum is the dominant blockchain used in DeFi,at 55% of the total value locked (out of over $200bn). Ethereum's share has however fallen from over 90% at the start of the year as Binance smart chain (BSC,now called BNB), offering much lower transaction costs,attracted many applications to be developed on

the BSC.

Many other new platforms have been launched in the recent years, to challenge Ethereum, two of which, Polkadot and Cardano, were created by co-founders of

Ethereum. Platforms are also competing for developers to build dApps.For example Cardano has launched, in collaboration with Wavemaker Genesis, cFund, which is a

$20m VC fund to seed projects building on Cardano with commitments of $250,000 to $500,000. Exhibit 12shows that Ethereum has been losing market share again more recently to Terra,a platform that manages its own stablecoin too.

How does DeFi compare to traditional, centralised finance?

There are multiple differences between traditional, centralised finance,and DeFi,

although DeFi enables some unregulated banking and financial activities, like for

example deposit taking.

Despite all these differences however, there are more interactions between DeFi and traditional centralised finance than investors often appreciate.

For example, DeFi relies on the AML/ KYC of banks to ensure that the

funds inserted in the system ("on ramps") are clean. Most importantly, we find it interesting to see that the most borrowed cryptocurrencies are stable coins - this shows that DeFi remains quite dependent on the Centralised Finance world.

DeFi protocols can become "centralised" when "whales" (large holders

of a specific token or cryptocurrency) control the voting power of a

protocol. This for example happened in 2019, when a whale holding

more than 90% of the voting power on Maker implemented a changed

that reduced the stability fee from 9.5% to 5.5%. Bitcoin is not centralised like some of

these DeFi coins and protocols

but there are elements of ownership centralisation as large institutions such as

exchanges and funds manage large cryptocurrency wallets on behalf of their clients.

Why DeFi?

A challenge to the financial system or a way to access leverage?

Defi proponents are pitching DeFi protocols as a way of improving the current financial
system. In reality, we have not seen DeFiexamples that effectively address these
concerns, rather this seem to us as a pitch to attract cash flow to enrich the protocol
operators.

Once we look at the pros and cons below together, our base case is that the DeFi

market will remain fairly small in the coming 2-3years,given the lack of regulation and

the nascent technology, which is prone to hacks or manipulation.

How could DeFi really take off?

In our view, the first key aspectneeded is more regulation, requesting more

"CeFi"elements to DeFi, in particular with respect to KYC, AML, resilienttechnology,

central entity to be regulated - this would make more institutional players comfortable in taking part in this market.

The current set-up of traditional finance has some shortcomings, which some DeFi protocols set out to fix, including, for example:

- trust based and dependent on centralised institutions (which DeFiaims to address by

doing away with intermediaries,although trust in a central entity is replaced by trust in a

smart contract)

- financial inclusion: there is unequal access,especially for those with the thinnest credit files, or new SMEs, or businesses located in developing economies

- intermediarycosts: the banking system is seen as an oligopoly with high barriers to entry due to regulatory licences needed - this translates into high fees, or bid-offer spreads

- liquidity inefficiencies: the oversupply of liquidity in one market often takes time to flow to the demand in another submarket

- legacyinfrastructure, which often prevents established players from being more efficient and thus cheaper

Yet we think a key component of the exponential growth of DeFi comes from the need for crypto traders to get leverage after being turned down for credit from traditional banks.For example, borrowing a cryptocurrency for a 10% annualised interest rate is acceptable to crypto investors as the cryptocurrency could be swapped for another that

may have rallied over 20%, making a strong return, if we are in a bull crypto market (see more on this in Use case #1:Lending and borrowing). In a bear market,however, this

ceases to work.

What are the risks and limits of DeFi?

While removing the central intermediaries might seem like a good thing at first, the trust

in the intermediaries is de facto replaced with trust in the technology on which the

smart contracts are built,and this brings multiple risks, which we would split into 1)

regulatory,2) market,3) technology, 4) operational and 5) personnel.

1. Regulatoryrisks

- financial crime: the lack of KYC / AML procedures implies high risk that DeFi

applications could be used to launder money;

- currently no availability of on-chain risk free asset to settle,although this might

change with central banks issuing CBDCs.

2. Market risks

- underlying assets are very volatile (except for stable coins);

- market manipulation can happen due to malicious miners.

3. Technologyrisks

- hacks: the audit process for protocols is not easy. Anyone can write a smart contract.

including with malicious intent;

- transaction costs,especially during periods of congestion,and scalability more broadly, especially if the underlying blockchain uses the "proof of work" method for validation;

- coding errors: large and irrevocable transactions that cannot be overridden can be dangerous, if they include coding errors. A protocol is only as secure as the smart contracts underlying it, but the average user will not be able to read the contract code, let alone assess its security;

- contract enforcement: while a blockchain contract may say that a person owns a house, only the police could enforce an eviction;

- forking, whereby open-source protocols can be cloned,and hence liquidity re-directed towards other,new protocols (as in the example of SushiSwap,a fork of UniSwap).

4. Operational risks

- concentration of governance tokens:governance tokens allow the owners to vote on a protocol's future. However, if ownership of tokens is concentrated in the hands of a

small group of malicious people,a protocol's credibility might be undermined,and funds might be lost;

- composability leads to dependencies: while composability is a great DeFi feature as it opens the door of financial engineering, it also creates dependencies,as users build

tokens on top of other tokens,and if there is an issue with one smart contract, this

might create issues to multiple applications across the entire DeFi ecosystem;

- external data dependencies: sometimes smart contracts rely on external data, which is not natively on-chain. This external data is provided by oracles,and this can lead to, potentially, centralised contract execution. This risk can be mitigated by using multiple

data provision sources,although this may not always be possible.

5. Personnel

- the code doesn't write itself, people write the code.

- as a result,a key risk is the goals and quality of the coding engineers.

- what is their intent? to truly address one of the perceived faults of the incumbent financial industry? or to create a platform to enrich themselves by creating a new currency,attract flows,encourage trading/transacting to obtain fees,and employ leverage to generate revenues? what is the business model they are building? is it sustainable or does it rely on continually increasing incomingnew flows to sustain its business model?

In relation to personnel, one key DeFi developer quit recently which will lead to a large basket of apps closing down in April. On 6th March 2022several cryptocurrency tokens sank on the news thatnotable developer Andre Cronje would no longer be contributing to the development of the DeFiand crypto space. On the back of this,around 25 apps and services will be terminated on 3 April 2022. Some of Andre Cronje's platforms had very high user growth, such as Solidly (a new project that went live on 24 Feb 2022, hitting $2.24bn total crypto value locked in three days)however platforms Fantom and Yearn Finance experienced the largesthit on price upon the news breaking. While it is too early to tell, this development may be signalling a peak in the DeFi industry,and more challenges to come, from more regulation and higher interest rates, for example.

Regulation: Key for the Development of DeFi The borderless nature of DeFi makes ithard to regulate. Decentralised Finance

protocols do not require the user to provide personal information that can identify them, which means that funds and transactions are harder to trace. In light of recent

limitations put on cross border holdings of assets and access to the banking system we may see regulators speed up their efforts to regulate cryptocurrency and decentralised finance platforms. Here are comments on DeFi from various regulators. United States

SEC Chair Gary Gensler said last year that DeFi projects are not immune to regulation. In particular as the SEC is focussing more on exchanges thathandle crypto transactions thatneed to be registered with the SEC. The difficulty is that the DeFi projects say that

they are not controlled by a central entity and don'tneed to be registered with

regulators. In September 2021 the WSJ reported that the SEC is investigating Uniswap, one of the largest decentralised exchanges. They are looking for information on "how Uniswap is used and how the team behind it markets the platform.". The investigation

seems to be ongoing but in January 2022the CEO of Uniswap said that JP Morgan decided to close his personal bank account. In November 2021, SEC Commissioner Caroline A. Crenshaw commented that the SEC looks to ensure that market activity, operates fairly,and offers all investors a level playing field,and this applied to DeFias well. She also said that "if DeFi development teams are not sure whether their project is within the SEC's jurisdiction, they should reach out to the Fed's Strategic Hub for Innovation and Financial Technology ("FinHub")".

Going through the opportunities and the risks presented by DeFi, she has highlighted the lack of transparency (as not everyone has the knowledge to read and understand the code a DeFi protocol is based on),and pseudonymity, which makes it difficult to know if

asset prices and trading volumes reflect organic interest or are the product of

manipulative trading by, for example, one person using bots to operate multiple wallets, or a group of people trading collusively.

The US Treasury commented in November 2021 on DeFi in relation to stablecoins, stating that digital asset trading platforms and DeFiarrangements present risks of particular focus to the agencies,and mostnotably to the SEC and CFTC. Areas of focus include risk of fraud; reliance of stablecoin arrangements on digital asset trading platforms such that a failure or disruption to the digital asset trading platform could threaten the stablecoin; money laundering;and excessive leverage.

US President Biden signed an executive order in March 2022to ensure responsible development of digital assets. Many different groups will produce reports on the crypto markets and their impact on the economy, financial stability and climate. Relating to DeFi, the executive order said: "Growth in decentralized financial ecosystems, peer-topeer payment activity,and obscured blockchain ledgers without controls to mitigate illicit finance could also present additional market and national security risks in the

future. The United States must ensure appropriate controls and accountability for current and future digital assets systems to promote high standards for transparency, privacy,and security – including through regulatory,governance,and technological

measures – that counter illicit activities and preserve or enhance the efficacy of our national security tools."

European Union According to Chainalysis,a cybersecurity and blockchain data company, Europe had the largest share of cryptocurrency transactions done via a DeFi protocol and the US had the largest USD value of transactions. The EU is due to vote on cryptocurrency regulations under the "Markets in Crypto-Assets Regulation (MiCA)

proposal", which may extend to DeFiand stablecoin regulation but the document doesn't explicitly

mention DeFi.

Estonia

Estonia is the only country we are aware of thathas introduced rules that effectively prevent decentralised finance platforms operating there. All asset exchanges need to register with the regulators as a Virtual Asset Service Provider and will need to be responsible for gathering identification of their users to adhere to anti-money laundering laws. Decentralised platforms don't require identification so cannot operate

in Estonia any more.

Global

In the past week, US, EU,and UK officials addressed the topic of cryptocurrency and economic sanctions – US' Elizabeth Warren and other senators wrote to Treasury Secretary Janet Yellen, the French Finance Minister Bruno le Maire said the EU would include it,and the UK's FCA reached out to crypto companies to make them aware of rules. In general, crypto companies, like exchanges,are being asked to register with

regulators such as the US SEC or UK FCA. They all will require users to provide

identification to sign up to follow anti-money laundering regulations.

What is clear is that the regulators have concerns about bank business or regulated type finance business occurring on non-regulated entities (as the CFTC Commissioner said in June 2021). KYC and AMLregulation is not followed on DeFiand transactions cannot be tracked in the same way as in traditional banking. It is not clear how the

regulators may conclude on how to implement regulation on these DeFi protocols which don'tnecessarily have a geographic location. Possibly institutional investors that are managing money on behalf of others who use DeFi protocols will need to report their large transactions. Any DeFi protocol that wishes to market products online may need to follow specific guidelines.

We will monitor the regulatory landscape closely,as its evolution will be critical to

determininghow DeFi can grow and expand from crypto only to mainstream finance.

Thefuture of DAOs. Many in the market are discussing whether a DAO structure is the new way of organising a company or raising funds. They have been very important for the growth of the DeFiecosystem,especially to incentivise new users at the start of a

project or to attract liquidity. This structure is interesting and has even become an employer for those who contribute to the growth of projects in return for crypto income.

DAOs may come under regulatory scrutiny as part of a discussion around the broader DeFiecosystem. There are a few aspects that regulators could be concerned with:

1) DAOs can be created by people or organisations only known by their pseudonyms;

2) DAOs can have retail or institutional investors so the risks needs to be properly known by that group;and 3) DAOs are starting to manage a large volume of assets (some over $1bn) so they could have to come under similar regulation as asset managers. As the creation of the DAO itself will be hard to prevent, we could see regulators looking to

prevent centralised crypto exchanges or companies from listing the governance tokens of projects offering very high returns.

Stablecoins

A stablecoin is a type of cryptocurrency where the creators aim for it to maintain a stable value versus something else, mostly the US dollar. Stablecoins have provided crypto traders a quick and liquid way to trade cryptocurrencies, like bitcoin and ether,as transactions stay within the crypto ecosystem which avoids the transaction and regulatory costs associated with trading into fiat US dollars through traditional financial

system. Stablecoins are the most frequently borrowed type of crypto asset on DeFi platforms as their lack of volatility provides a good basis for trading and lending contracts. Currently around half of all bitcoin and ether traded on all exchanges is versus a type of stablecoin, making it important for both the centralised and xdecentralised crypto ecosystem.

Therearetwo main types of stablecoins - asset backed and algorithmic. Of the asset backed, most are fiat currency asset backed (US dollar),a few are commodity backed (gold) and some are cryptocurrency backed. The two largest stablecoins (USDT and USDC) are US dollar asset backed but are also considered to be centralised stablecoins.

Asset backed stablecoins rely on the market's trust that the issuer has liquid assets that can be sold and used to defend the value of the stablecoin in times of market stress.

The lack of transparency around the reserves that back Tether (USDT)have caused some concern.

The DeFi world particularly utilisesalgorithmic stablecoins (such as DAI), which are decentralised stablecoins. The money supply is controlled by an algorithm to keep the

coin's value stable. Consider the algorithm like a central bank controlling day to day liquidity based on predefined rules. If a stablecoin is managed versus the US dollar then

in theory its purchasing power should be equivalent to the US dollar. Within DeFi, stablecoins are traded through liquidity pools and borrowed through lending platforms.

Regulators are focussed on the issuers of fiat-backed stablecoins but similar to DeFias a whole, it is not clear if they can practically regulate the algorithmic stablecoin protocols.

Largest stablecoin

The two largest are Tether (USDT) and USD Coin (USDC), which is issued by Circle, covering over three quarters of the stablecoins out

there. Justunder $50bn of USDT crosses traded on cryptocurrency exchanges in the past day, or around 59% of the USDT cryptocurrency in circulation.For comparison, $1.7trn of USD was traded in fiat currency spot markets a day in 2019 (latest available data), or 30x that of USDT. Over the past year, circulation of USDC has been rising, taking more of the stablecoin market share,now at 28% of the major coins.

Terra USD (UST)has become the largest algorithmic stablecoin by market cap with a 7% share.

Stablecoin lending – just like banks?

Cryptocurrencies can be borrowed from a variety of centralised (CeFi) and decentralised (DeFi) platforms. Centralised lending is where participants trade with the crypto company as their counterparty and decentralised lending is where participants use smart contracts to link depositors and borrowers directly. US regulators have recently started limiting the products that centralised lenders can offer but decentralised lending has not yet been stopped. We would expect regulation to also limit DeFi lending at some point.

In January 2022, it was possible for a US resident to deposit USDC, a USD based stablecoin, into an account with BlockFi and receive 9.5% annualised interest, paid in USDC. The interest rate was much higher than fiat USD deposits in a US commercial bank, which caught the eye of regulators, as the risks associated with this type of product are very different. In February 2022, BlockFi was fined $100mn by the US SEC for not properly registering its high interest deposit products and disclosing the risks for the depositors as they were dealing with securities and not currencies. BlockFi will no longer offer these high interest accounts for US residents and other companies like Nexo have also discontinued their deposit products. We expect centralised crypto

lending products to continue to be offered by a variety of companies but that these companies will need to be registered in a similar way to securities isssuers.

The largest decentralised lenders of stablecoins are Anchor, Aave and Compound. As described in other sections above, most decentralised lending is overcollateralised, so

the borrower will need to deposit collateral in another cryptocurrency, with a value higher than the value of crypto they wish to borrow.Following BlockFi's fine from the SEC, Circle the issuer of USDC decided to delay its introduction of a DeFi product, citing a need for more regulatory guidance and enhanced compliance tools.

Algorithmic stablecoins – a DeFi use case

DAI has become one of the most popular stablecoins on decentralised finance

platforms. DAI is not asset backed but is a form of algorithmic stablecoin, where coins are created and destroyed via smart contracts to balance the value in the market.For example if the price of DAI moves above $1, DAI are created to increase money supply and reduce the market price. On a day to day basis,a system managed by MakerDAO

allows users to deposit cryptocurrency as collateral (e.g. ETH or ETH-based assets) and receive DAI as part of a smart contract,known as a collateralised debt position (CDP).

Algorithmic stablecoins have the advantage of transparency, which makes them easily auditable,and that the related applications are decentralised.

More details on how DAI is created. DAI is related to the Maker DAO protocol. Anyone can use Maker to deposit collateral such as ETH or BAT in a vault and generate DAI as debt against that collateral. The owner of the DAI debt will incur a fee known as a stability fee which is continuously accruing interest and paid upon repayment of borrowed DAI. The concern with managing the stable value of the DAI vs 1 US dollar is what happens on days when crypto markets are down and so the collateral's value declines quickly. Users can only borrow DAI up to 66% of their collateral's value (150%

collateralisation ratio). If the vault's value of the collateral falls below that ratio then apenalty fee has to be paid of 13%,as well as liquidation of the vault.Liquidated

collateral is sold on an open market at a 3% discount. Generally the system has worked well but like with all stablecoins, DAI has seen volatility with its price going as high as $1.10 and as low as $0.95. Adjustments to the fees have been able to stabilise the coin.

An alternative type of stablecoin is partasset backed and partalgorithmic, such as FRAX. The Frax protocol has created two tokens - a stablecoin called FRAX and a governance token called Frax Shares (FXS). The protocol also has a pool contract which holds USDC collateral. Pools can be added or removed with governance. The developers hope to increase the part of the stablecoin that is backed by an algorithm so that it becomes a larger share over time as more users come to the platform.

Risksaround algorithmic stablecoin valuations. Users of decentralised stablecoins assume that the algorithm is robust enough to manage the stablecoin's value in times of market volatility and uncertainty. Many algorithmic stablecoins are created through deposits of another cryptocurrency and with smart contracts managing the supply and demand. Sometimes if the code is not well developed to manage liquidity in times of

market stress, the valuation of the stablecoin can fall quickly.For example Iron Finance's token called Titan dropped to zero earlier this year due to its poor stability mechanism and weak underlying assets that backed it. Overcollateralized stablecoin creation (e.g. 1

ETH creates 0.66 DAI)helps to manage these types of risks.

Stablecoin regulation is coming

Centralised stablecoins issued by private companies/groups are competitors to the US dollar and related banking system. Transactions in the banking system are monitored by central banks, regulators and government authorities and the money supply is managed by them too. In recent months, there has been heightened focus on how to regulate

stablecoins, with the US president's working group (PWG) proposing that certain stablecoin issuers should register like banks. That would mean they need to provide updates on the reserves that back the stablecoins. Stablecoin related bills are expected to be introduced into the US house and senate in the coming month. The PWG proposals are for asset backed stablecoins, it is not clear to us at this stage how they would regulate algorithmic stablecoins as technically they don'thave one central company/issuer.

What should we expect?

Should global regulation follow some of the guidelines suggested in the reports above, then we would expect there to be two types of stablecoins in the market – regulated and unregulated.

At the moment, we think regulated stablecoins would gain market share and usage amongst the institutional investor community. The unregulated would likely be more popular among the retail investor community. Using bitcoin as an example, the liquidity of bitcoin to regulated stablecoin crosses could end up beinghigher than that with

unregulated stablecoins.

Regulations are unlikely to be global but there are likely to be similarities between how the developed economies treat stablecoins (e.g. USA, Eurozone, UK,etc.).

The type of questions being asked by regulators around the world currently are:

1) Is a stablecoin a security?

2) Are payments allowed on a public blockchain thathas only a wallet address as an identifier? Do all transactions need to be tracked?

3) Should cryptocurrency companies be allowed to offer deposits and lending facilities that emulate banks?

Currently stablecoins are only used in the cryptocurrency world and there are few examples of their use to buy goods and services. If we do end up being able to pay online retailers using stablecoins to receive goods, does that mean that consumers would prefer that system of payment over the current system using the banks and credit/debt cards? Would the technology be that different from a users' perspective if that transaction were tracked and monitored via the merchant?

A question for thefuture: could weend up ata place wherestablecoins plusassociated blockchain technology will evolveand be used byso manythat central bank digital currencies will adopt thetechnology? There are a lot of roadblocks to this outcome including privacyand legal concerns

Use Case #1: Lending and Borrowing

Summary

How does this DeFi product comparevsexistinglendingat banks?

Rather than something similar to traditional lending, for now we see these type of loans as more akin to cross-currency swaps, because the DeFi platform is lending one crypto against another. We could also consider these loans to be more like securities lending, as investors are pledging one crypto for access to a different crypto.For this, we need to think about cryptos as assets rather than currencies. At present we don't see DeFi technology impacting the incumbent industries.

We could see how DeFi lending protocols could be applied to other forms of collateralised lending thathave multiple trigger points for borrowers and lenders.For example, mortgages is an asset class thathas various trigger points including LTV, borrower DTI, mortgage insurance, title,appraisal,etc. Encoding all the relevant borrower details,valuation details of the property,and, most importantly, that the mortgage is enforceable could make DeFi technology useful here. The challenge however is that all parties to this contract would need to adopt the protocol, including the legal system (i.e.,a contract may say that a person owns a house, only the police could enforce an eviction),and at this stage it seems more likely to us that mortgages evolve to a more digitalised form, rather than experience a complete change of the infrastructure on which they run as would be the case if using DeFi.

While mortgage lending via DeFi may be difficult centralised crypto options have been considered.For example United Wholesale Mortgage in the US trialed crypto-based mortgages buthave decided not to go ahead due to low demand and regulatory hurdles. The mortgages would have gone via the centralised system run by the

broker, justusing cryptocurrency as the currency, so we could call it a full CeFi crypto system.

As the key function of credit risk assessment is currently missing from the DeFi lending and borrowing products,and it is substituted by an overcollateralisation of positions, we struggle to see how these products could for example replace corporates or unsecured consumer lending,unless there is enough reliable data given to the protocol. We should mention that there are some protocols (for example Teller, TrustToken and Maple Finance) that claim they do uncollateralised financing in DeFi, but we think all of these have either some elements of centralisation, making itnot very "DeFi" but rather more "CeFi" (for example they ask for a physical address,and bank account statements), or overcollateralisation (for example, TrustToken states that before giving a loan they check that the borrower has available liquidity in the form of unencumbered liquid assets and collateral coverage that may range from 10.0x to 15.0x the total loan amount).

Why are crypto lenders offering higher rates on USD stable coins vs USDsata bank?

Cryptocurrency traders and new companies have often found it difficult to borrow from traditional banks. Banks consider cryptocurrency risky and may have been worried about reputational risk associated with such a loan. So crypto borrowers turned to the crypto markets. The demand for such borrowing in a market with relatively low liquidity

versus the traditional banking system, kept interest rates on USD stablecoins higher than USDs in the USD banking system.

Why has there been demand? As an example, even if the borrowing rate is 5%, in a cryptocurrency bull market, it has been possible for the trader to convert the borrowed stablecoin into another cryptocurrency and earn a higher return (e.g. 10%) on the price appreciation. Crypto borrowing demand is high in a cryptocurrency bull market, which tends to occur when global availability of liquidity and credit is also high. We would

expect cryptocurrency borrowing to slow in a bear market. Note that the borrowing demand has come from both centralised (e.g. BlockFi, Nexo) and decentralised (e.g. Compound, Aave) lending platforms. Are there any examples of incumbents institutions experimenting with these platforms? Societe Generale has proposed a $20M DAI loan in exchange for bond tokens. CoinTelegraph reported on 30 September 2021 that the digital assets division of

Societe Generale (Forge) has submitted a proposal to the governance forums of

decentralised finance platform MakerDAO to provide covered bond tokens (obligations de financement de l'habitat or OFH tokens) as collateral for a loan of the DAI stablecoin.

We note that while the proposal is publicly available on the MakerDAO forums, Societe Generale has not commented on this report. If confirmed, this would mark the first major collaboration between a traditional bank and a DeFi protocol, and would bridge the gap between centralised and decentralised finance.

Technical details

There are two types of loans so far in DeFi.

1) Over-collateralised loans

A borrower is required to post collateral,exceeding the value of the debt. In case the value of the locked collateral falls below some liquidation threshold, so-called liquidators,a type of keeper,are able to purchase the locked collateral at a discount and close the borrower's debt position. In a liquidation scenario, the liquidated borrower would receive the collateral minus any outstanding debt and incurred penalty charges.

Over-collateralisation doesn't translate in to the loans being fully risk-free, because for example in times of financial crisis with thin and illiquid markets it could be unprofitable for liquidators to initiate liquidations. Separately, if the borrowed assethas endogenous price effects, for example because its price is impacted by other agents' decisions in the

system (as is the case for Dai), forced liquidation could result in a spiral effect on prices (see the case of Dai's "Black Thursday"). Although these contracts are called "loans", we would characterise them as more akin to swaps.

Flash loans

Flash loans were first created in 2018 by a company called Marble but they became popular when introduced by Aave in early 2020 on Ethereum.Flash loans are not collateralised but they last the duration of a single transaction, with the borrower

having to repay the full borrowed amount plus interest by the end of the transaction - if the borrower doesn't repay the loan, then the transaction fails and it is cancelled,and it is as if the amount was never borrowed at all. These type of loans are typically used in arbitrage swap.

Interest rates are set based on protocol-specific interest rates models,and are calculated by smart contracts according to demand-supply dynamics. As an example, we look more closely below at Aave, one of the leading lending protocols. The other two most famous are MakerDAO and Compound.

Use Case #2: Exchanges

Exchanges like the LSE and DB1 are centralised as an intermediary provides accurate price information, matches buyers and sellers to process trades and settle transactions.

Similarly, most cryptocurrency exchanges, such as Coinbase and Binance,are centralised.

Centralised exchanges are fairly efficient and work pretty well,although they present two potential issues. The main downside of a centralised exchange is the need to deposit some assets with the exchange before trading, thus losing access to these assets,and having to trust the exchange operator. Secondly, centralised exchanges, like all

centralised financial institutions, represent a single big target for hackers,although there haven't been material cyber attacks to date on large established exchanges.

Decentralised Exchanges (DEXs) are digital asset trading platforms that rely on smart contracts to enable users to conduct automated transactions without a centralised authority. Contrary to centralised ones, DEXs leave the users in full control of their assets until the trade is executed,given they facilitate the non-custodial exchange of

onchain assets,and the execution happens atomically through smart contracts, meaning that both sides of the trade are performed in one indivisible transaction,and this mitigates counter party credit risk. All trades are settled on-chain, which ensures the

public verifiability for all transactions to network participants.

One interesting feature vs the current infrastructure, in our view, is the atomic

settlement and on-chain trading - yet,a recent experiment by Euroclear, the French Central Bank, the French Treasury (which we have written abouthere)has found out that the best time for settlement would be T+0 end of day,as market participants would still be able to benefit from intra-day clearing and netting withouthaving to bear the additional capital and margin costs for any extra day delay.

DEXs can be structured in different ways, such as:

- order book DEXs (which have individual or batch settlement), on or off the blockchain

- constant function (automated) market makers, AMMs, which dynamically adjusts prices and executes trades based on available liquidity,and does away with the order book altogether.

These exchanges offer not only cryptocurrency trading, but also asset and derivatives.

While Uniswap, Sushiswap, PancakeSwap and Curve are the most famous DEXs, we counted multiple others,and we have looked at more than 30 for this note.

Other Use Cases:

Derivatives, Portfolio Management, Wallets and Insurance Decentralised Finance goes beyond lending, borrowing and trading of cryptos,and extends to the broader spectrum of financial services, including derivatives, portfolio

management, wallets and insurance for example. While not the focus of this note, we provide a quick overview below.

Decentralised Derivatives are tokens that are typically either asset-based, i.e. derive their value from an underlying asset's performance, or event-based, i.e. derive their value from the outcome of the event, or the development of any other observable variable (for example a sporting event or the weather).

An interesting case of asset-based tokens are inverse tokens, which allow a user to get short exposure to cryptoassets, i.e. their price is determined by an inverse function of the underlying assets' performance.

The most famous derivatives protocol is Synthetix, but we have counted more than 20 other protocols.

Asset Management

While in traditional finance investors rely on asset managers to manage and allocate their portfolio, in DeFi,asset management protocols invest through smart contracts into "vaults" or "pools", in a variety of tokens, digital assets, or interest-bearing accounts.For example on Set Protocol, perspective investors can choose amongst "thematic" baskets, for example a Metaverse Index (including tokens in the entertainment, sports and

business shifting to a virtual environment),a Data Economy Index (including tokens that provide data-based products or services across blockchains),etc.

Incomefrom crypto staking

Some crypto applications may also stake cryptocurrency for the user, providing the

staking rewards or other tokens in return. These applications are not truly decentralized

and so we wouldn't classify them as DeFi but the tokens they create are used on many

other DeFi applications and so are an important part of the ecosystem.

LUNA has the largest value staked at $31bn, or 41% of the market cap of LUNA. The

token is associated with the Terra blockchain, which has become an increasingly

popular venue for DeFiactivities. According to Staking Rewards, staking LUNA offers a

reward income of around 6% annualised.

Some crypto applications offer users the ability to stake their cryptocurrency holdings,

like a deposit in a bank account, then offer the user another token that represents the

value of the cryptocurrency they deposited. The advantage is that the user can benefit

from the income received for staking but also not lose the ability to sell an asset in

times of market stress,especially as staking requires users "stake" their crypto for

extended periods of time. These are known as liquidity tokens, the largest of which is

called sETH, created through users depositing ETH with Lido.

Wallets

Wallets are the first DeFi touchpoint for users,as they are mobile apps that allow users

to interact with dApps, store private keys,and view balances and holdings. Notable

Examples are Metamask, Dharma, Pillar. Wallets are typically non-custodial,as in users

are responsible for storing funds and assets withouthaving to rely on a financial service provider (private keys and passwords are stored locally on the device). Yet, losing the password or the mobile can lead to loss of funds, which is a main hurdle to adoption.

Insurance

As discussed earlier, DeFiapplications are based on smart contracts. As a result,

vulnerabilities in the code of smart contracts will have a negative impact on the DeFi services. Insurance in DeFienables users to hedge against bugs in smart contracts. The most prevalent insurance protocol, Nexus Mutual, offers insurance on specific Ethereum

applications. Hence, consumers can have smart contract protection for their funds lent on Compound or money invested in Uniswap. Insurance in DeFi space is still in the early stage, but ithas potential to grow beyond smart contract insurance in the future.

DeFi in Context

DeFi is one of the earliest and fastest growingniches within the decentralised Web3 ecosystem. DeFi enables web-based communities to exchange value via a local currency.

The main benefit is to the owner of the community as they can set exchange rates, transaction rates, minimum entrance fees, loyalty points,etc. While this could be done via fiat as well, the profit potential is higher when you are your own central bank that lacks competitors.

DeFi is,however, only one part of the web3 adoption narrative. Below we present a chart gallery which should allow investors to better understand DeFi's growth relative to other industries that are also seeing the adoption of decentralised applications (DApps) and platforms where peer-to-peer user inaction are a key feature.

DeFi currently has the highestuser base per DApp as well as highest volume traded across the industry. Despite this, marketplaces,gaming,gambling, media, marketplaces and social platforms are seeing,albeit from a lower base,higher growth rates in the numbers of DApps launched as adoption of the technology accelerates.