UNIVERSITÀ DEGLI STUDI DI TORINO

DEPARTMENT OF MANAGEMENT

BACHELOR'S DEGREE IN

BUSINESS & MANAGEMENT

THESIS

DEFI: THE RISE OF A NEW TOUCHLESS ECONOMY

Supervisor: GAY Mario

Candidate: MAMINO Matteo 894709

Academic year 2020/2021

INDEX

INTRODUCTION

Bitcoin, 2009, its inception is the key enabler of a new concept in financial industry, decentralization. For the very first time the idea of personal banking has a real and practical development. In 12 years a lot of research and innovation have built what in 2009 seemed just an utopistic reality. Numerous project have improved the capacity of blockchains and have implemented all sort of use cases, from the smart contract of the Ethereum blockchain to the oracles of Chainlink, all this effort come together to finally build a new and constantly growing financial world, the DeFi or Decentralized Finance. DeFi is built upon disruptive innovations such blockchains and smart contracts which allow users to be in direct control of their personal financial management, avoiding traditional centralized entities (banks). New opportunities for both rich western countries and poor and undeveloped countries, sustaining the concepts of “unbanking the banked” and “banking the unbanked”. It's important to fully understand all the aspects of DeFi, starting from the needs that aim to satisfy, to all the services that it is already offering to its users, such as landing and borrowing, insurances, decentralized exchanges and so on. The paper will also process a meticulous comparison between the traditional financial world of banks and this new decentralized reality, considering the geopolitical implication of such change. The research goal is to understand how much influence DeFi could have on the future of the financial industry and also the impact that could have to mankind’s progress.

1. DECENTRALIZATION BASICS

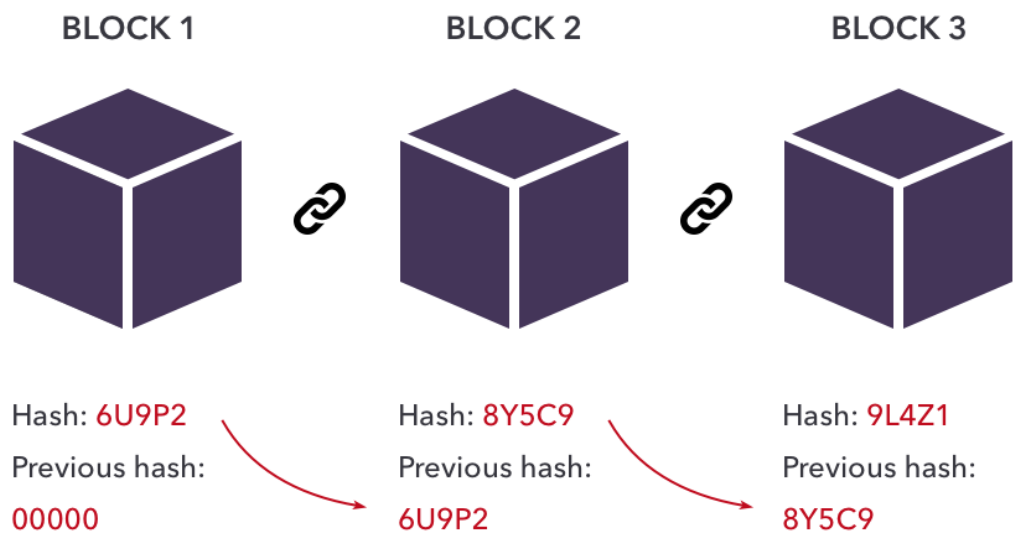
In order to completely understand Decentralize Finance (DeFi) there is the need to take a step back and analyze what decentralization means and where it comes from. To answer these questions, we need to dive deep into the technologies that constitutes the foundations of this new and innovative concept.

1.1 Blockchain

The blockchain can be considered as a database, but it stores information in a unique and totally different way. It must not be analyzed as just a simple "new technology", it doesn't create just new functions and it doesn't satisfy just a couple of needs like the most of products, the blockchain technology introduce a completely new paradigm. Let's look at the last 30 years of innovations, Internet came up during the 90's and totally disrupted in less than two decades the global society.
In the subsequent years, the biggest change that internet brought to the public was dematerialization, over the time, more and more thing passed from a physical existence to a complete digital one. Amazon dematerialized retail, Google dematerialize information, iPods dematerialized music and now, after the incredible revolution of internet, for the first time in human history, the blockchain technology give us the possibility to dematerialize property.
What does it mean? And how does blockchain make it possible?
To fully comprehend the real opportunities of this technology, we need to figure out how a blockchain works and how it's composed.
Structurally speaking, the blockchain can be visualized as a net made from components called nodes or blocks. The behavior of the entire system is determined by the behavior of each single node. The concept of decentralization has seen its creation in these principles, the net is not controlled by any centralized entity, the network is managed and moved by the interactions between nodes.

The blockchain continuously grows, adding new nodes, and right in this process its immutability and security features come to life. Every node contains transactions information, when it has no memory left, it generates a new node. Let's assume there's a block "A", when it runs out of memory, the node's data (input) pass through a mathematical algorithm which transforms the original information into a new string of data called "hash" (output). This process is unilateral, it's almost impossible to get the input information from the output (hash), the only way to do it, it's by taking random tries, that with a high cryptography level, could be translated into millions and millions of attempts. Now it's clear how every node is linked to the previous and next one, it's also evident the meaning of "immutability", a node manumission would require an enormous computational power, which is not reachable with currently technologies.

Cryptography principles



SOURCE: ig.com

These are the basic logics behind the nature of the blockchain, now it's important to understand that an ecosystem like DeFi needs something more than just the basics.

1.2 Blockchain 2.0

In 2015 a new blockchain generation went live, the Ethereum blockchain. More complex than the previous and basic form, the Ethereum one offer functionalities such as the possibility to develop decentralized applications (DAPPs). This function opens the door to thousands of different use cases, fixing the point of start of DeFi as we know it today. Its invulnerability to hackers' attacks and its multifunctionality have opened the possibility to use it as a storage for important companies' databases and private information.

The biggest integrations of this new blockchain generation are the smart contracts. They are decentralized algorithm, built with a programming language called "Solidity". They run when predetermined conditions are met, with simple concepts like "if/when … Then …" their execution could result in exchange of asset, enforcing private protection, lock of funds and so on.

Smart contracts totally deleted the need of intermediaries, allowing financial agreements between users, without discriminations and time-wasting activities usually part of centralized networks.

When a smart contract is used, all the blocks verify the results, certifying them.

The advantages brought are clear, from cost efficiency to processing speed, without forgetting the reliability factor, removing potential human error, and adding a great precise execution.

There's no financial system without money, how do money work in the decentralized world of blockchains?

When we talk about money, the most important aspect is the fungibility, which means that all units are identical and mutually interchangeable, the dollar in your pocket is completely identical to the dollar in the cashier hands, which is also identical to the dollars printed by the U.S Treasury Department. There are also non fungible assets, like diamonds, each one is different from the others according to variables like the dimension and different physical characteristics.

The same concepts also apply in a decentralized world.

There 3 main types of assets on the Ethereum blockchain:

- ETH: It's the native fungible token of the Ethereum blockchain, which means its information are intrinsic to the underlying structure.
- ERC-20 token: It can be considered as a non-native token because it's just a smart contract with a database inside. It contains a list of requirements that a programmer needs to fulfil in order to create a non-native fungible currency on the Ethereum blockchain. The ERC-20 token is the standard of some of the well-known cryptocurrencies (LINK, USDT, MKR)
- ERC-721: This token standard brings non fungible assets to the Ethereum network, ensuring that distinctive details about an asset can be immortalized. Also called NFT (Non-Fungible Token), fits perfectly with the property requirements of a one-of-a-kind artwork, leveraging the ownership and immutability principles of the blockchain.

2. DEFI

DeFi (Decentralized Finance) is a set of applications which build a complex and rich ecosystem that aims to create a new financial world, open to everyone, which doesn't require to trust any type of intermediaries.

As I explained in the introduction, DeFi strongly relies on cryptography, blockchain and smart contracts.

Most of the DeFi applications are built on top of the Ethereum blockchain, which is also home of ETH the second most valuable cryptocurrency by market capitalization.

The main reason behind the need of the Ethereum technology is the capability to build complex and efficient smart contracts through its programming language "Solidity" which allows the programmer to fulfill all the logics required from the DeFi Dapps.

The smart contracts added the concept of programmable money. With them, the ways of managing assets are practically endless.

Just like the traditional financial system, the Dapps offer many types of products and services such as borrowing and lending, trading, and exchanging, liquidity and so on.

To showcase DeFi in the best way possible, I want to disclose and analyze all the basics of how a financial institution works.

The main characters are of course the banks. But why are the banks so important?

First, we need to understand that the traditional financial system is designed to support growth in economy, creating ways to allocate capital.

Without banks, the access to credit would be almost impossible and much riskier, small businesses won't be able to finance their activities, normal people won't be able to buy a home and build a family around it. Of course, banks bring a lot of benefits to our society but not without any types of risk. First, banks set the system at their own rules, that are prone to human related risks such as mismanagement and corruption.

The global financial crisis of 2008 is the clear evidence of all the problems that banks can create because of conflicts of interest and bad management.

The crisis exposed the inefficiency of the traditional financial system and it's definitively not a coincidence that "Satoshi Nakamoto" gave birth to Bitcoin right in those years.

The new-born stage brings some compromises, the technology can’t allow a totally and efficient decentralization yet. That’s why the access to the crypto world, now, sees its biggest inflow of users on centralized platforms, such as Binance, Coinbase, Blockfi and Crypto.com.

These kinds of realities can be considered as hybrids, they got services and opportunities of DeFi but are launched and managed by centralized entities.

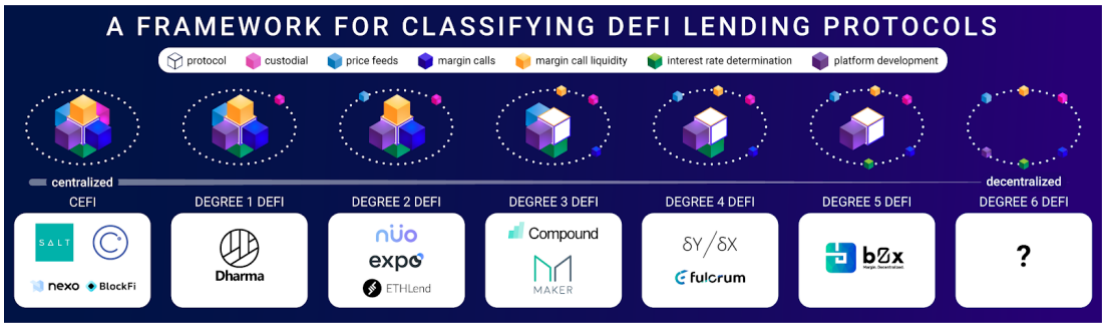
The decentralization grade can be evaluated by looking at variables like the custody of private keys, the determination of interest rates and price feeds, and in which direction the platform development is oriented.

In the current state, no DeFi protocol is completely decentralized yet.

DeFi’s rise preserves and reinforces the crypto ethic of trustlessness, reforming an ecosystem that was falling prey to centralized control.

A multi-layered analysis of the ecosystem is the best thing we can do to fully understand the wide variety of applications and services.

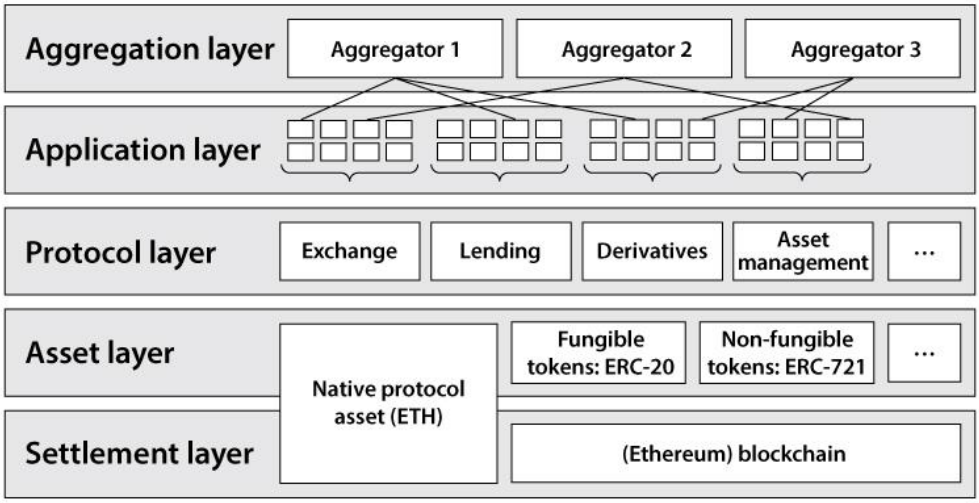
How decentralized is DeFi?



SOURCE: medium.com

2.1 Ecosystem

DeFi layers



SOURCE: On Blockchain- and Smart Contract-Based Financial Markets, by Fabian Schär

The shared and complex infrastructure of the blockchain gave the possibility to programmer and developer to build a detailed and boundaryless ecosystem that can be divided into 5 main layers.

The settlement layer is represented by the blockchain and its native protocol assets (ETH is the native protocol asset of the Ethereum blockchain). It's the layer where the ownership information are securely stored. The blockchain is the foundation of the entire ecosystem.

The asset layer consists of all the assets that are issued on top of the settlement layer, this is home of the native protocol assets as well as any assets issued on the blockchain (non-native assets).

The protocol layer is of course the one we are going to dip more into, due to its user related application and its direct comparability to our traditional financial system. It provides standards for specific use cases such as stablecoins, decentralized exchanges, derivatives, landing and borrowing and so on.

The application layer and the aggregation layer are strongly related to each other, and both consist in user-oriented interfaces and applications, which are created to ease the access and use that otherwise would have been complex and difficult.
Thanks to this type of interoperability, the ways of allocating and managing funds are practically endless, that's why DeFi is often called money LEGOs. Users can combine services, juggling between all different protocols, trying the solutions that best meets their needs. Unlike the traditional financial system, DeFi allows the user to stack multiple product and services on top of each other, complementing all the benefits of each protocol.

2.2 Yield farming

When the bond market is not good, there's always a hunt for yield, and DeFi, with the lending & borrowing protocols and stablecoins, built the perfect ecosystem, interest returns from 2% to 12% and the volatility control of stablecoins.
It's undoubtedly one of the most researched use cases in DeFi. As the name suggests, yield farming consists in lending crypto assets in order to generate high returns, the interests are then lent again, gaining the compound factor and leveraging even more the investment. The "farm" is constituted by the yield opportunities, and users jump from a protocol to another one to find and exploit the best "farms".
The interest rate used to measure these kinds of returns is APY which means Annual Percentage Year and represents a compound interest.
The DeFi ecosystem represents the perfect environment for yield hunting, with all the varieties of protocols and platforms that combine different service and products together.

3. DEFI SECTORS

Now that we have a clear view on how the DeFi ecosystem is structured, we can directly dive on analyzing the different protocols and use-cases offered by this reality.

3.1 Stablecoins

Stablecoins are cryptocurrency linked to an asset like the U.S. dollar that doesn't change in value, they attempt to fill the gap between fiat currencies and cryptocurrencies. The entire topic strongly relies on concepts such as volatility and price stability, what are those concepts? And which relations do they have with stablecoins?

Price stability is obtained through a high liquid market and through the control of the supply by a regulator.

In the other hand, volatility is obtained when the market is highly illiquid, which means that a single buying/selling transaction can have a big impact into price level, and when the supply amount can't be adjusted by a regulator.

It's clear now why the cryptocurrency market is volatile, there are no regulators who can adjust the supply of currencies and there is not enough liquidity to guarantee price stability during selloffs.

Two main reasons for the price stability of fiat currencies are the reserves that back them and the market actions by controlling authorities, like central banks. Since fiat currencies are pegged to an underlying asset, which act as collateral, their valuations remain free from wild swings.

The majority of stablecoins that currently exist use the dollar as their benchmark asset, but many are also pegged to other fiat currencies issued by central banks like the euro and yen.

There are 4 types of stablecoins:

Fiat backed: Also called IOU (I owe you), you deposit fiat currencies to get the same amount in stablecoins, with the right to redeem your fiat at any time. The fiat deposit implies a centralized regulator, the perfect examples are USDC, issued by the company Coinbase and BUSD, issued by Binance.

Crypto backed: obviously backed by crypto assets, as I already explained these assets don't have the same price stability as fiat currencies so to maintain a fixed value, the stablecoins are over collateralized. The absence of fiat allows the creation of a decentralized and unbiased ecosystem. That's exactly what MakerDAO did with the creation of DAI, the most famous and used decentralized stablecoin.

Precious metal backed: have the same main characteristics of fiat backed, but instead of reflecting the price of a fiat currency, they reflect the price of the precious metal that it's backing them. As for fiat backed, these of type of currencies need an issuer/regulator.

Algorithmic: the token supply is managed by an algorithm which burns tokens if the price is falling and issues new tokens if the price is increasing too much.

Thanks to their peculiar characteristics, these coins allow users to access different types of strategies and services.
The lending is an important aspect of the DeFi ecosystem and with stablecoins become even more desirable. For example, at the start of 2020, the US 10 years treasury bonds had a yield around 1%, and the returns compared of lending stablecoins is between 2% and 12% APY (Annual Percentage Year)
You have the possibility to earn interest on your crypto deposits, interests way higher than those offered by banks.

3.2 Decentralized Exchanges (DEXs)

As the traditional financial system has banks, DeFi has decentralized exchanges. They work thanks to smart contracts, and they totally deleted the role of intermediaries. DEXs allows crypto investors to trade and exchange crypto assets while holding their key and maintaining the reason of decentralization.
There are two main types of DEXs:

Order books: they usually belong to centralized exchanges (CEXs) like Binance and Coinbase, but it's important to also explain this topic to deeply understand the meaning of decentralization.
DEXs with order books are not usual due to the liquidity factor, users may have to wait a long time before having their order filled, instead, CEXs have usually much higher volume and liquidity.
Order books basically keep track of all the on-going trading activity, they display multiple different charts which allow the users to set up strategies based on data analysis.
They also offer the possibility to place limit orders, this function it's particularly useful for those who are not active traders.
Up to now seems that order books on CEXs are the perfect solutions for a crypto investor, their services are reliable, cheap, and efficient, but all these pros at the cost of decentralization, indeed in CEXs, the crypto-assets would be held on the exchange platform whereas for DEXs, crypto-assets for trade would be held on users' own wallet.

Liquidity pools are token reserves locked up in smart contracts.
The liquidity is provided by users called liquidity providers who are incentivized by APY interest rates (annual percentage year) that most of the time are fed by transaction fees that users pay to access the exchange services.
Usually, each liquidity pool represents a trading pair, for example, ETH/BTC, USDT/ETH and also pairs between stablecoins like DAI/USDT or USDC/BUSD.
The most famous DEXs are Uniswap and SushiSwap correspondingly $6,45B and $4,05B of liquidity locked up.
How these Decentralized exchanges work?

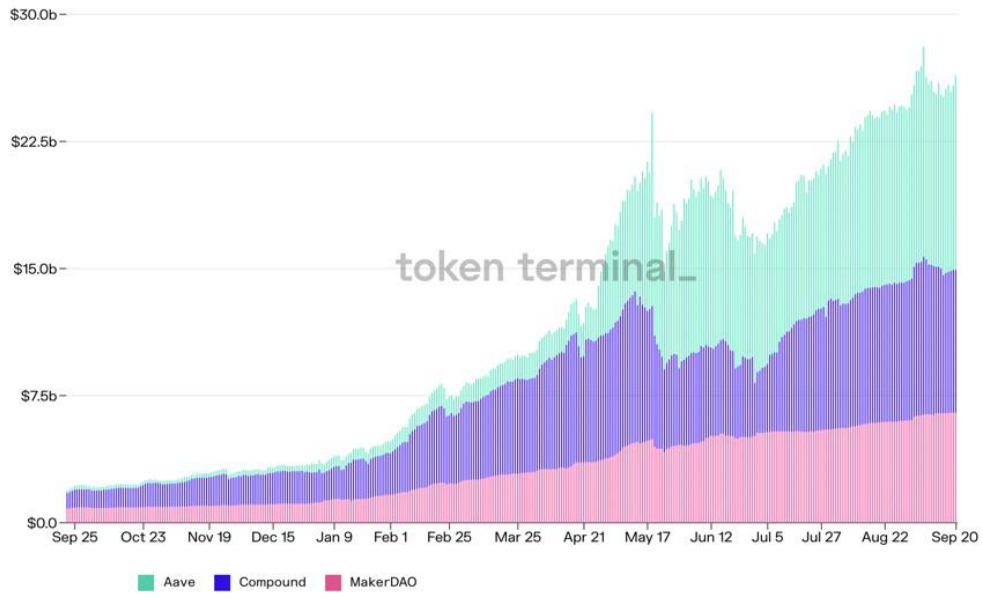
Users can exchange tokens accessing the liquidity pool of their interest, for example using ETH/USDT trading pair with 100 ETH and 335 000 USDT in the liquidity reserves, a user wants to buy ETH selling USDT, he would send 3350 USDT (current ETH price) to the Uniswap smart contract to get 1 ETH in return. After the transaction the pool is left with 99 ETH and 338 350 USDT.
The ratio between the pair determines the price of the assets, this operation is led by the Automated Market Maker Mechanism (AMM).
AMM algorithmically determines the price of crypto assets in a specific pool, maintaining constant the product of both assets.
Obviously now, when we add or subtract an amount to one of the two assets, the price of the other will be determined asymptotically.

3.3 Decentralized lending & borrowing

One of the foundations of our global economy are of course the money markets. Most of the economic activities would not even exist without money markets, even the biggest company of the world would not exist, that because these types of markets offer the possibility to access funds in the earliest stages of company foundation, allowing economic activities to start.
Usually, funds are accessible through the traditional financial system, which request a certain level of trust, earned through collateralization, and with intermediaries, which is a role taken by the banks.
This type of systems has been around since the creation of the first trading activities, and it has permitted the proliferation of wealth and well-being all around the globe, but it has also led to major problems and shortfall that can’t be accepted today anymore. Problems such as geographical discrimination, restrictive funding criteria and the exclusivity of rich groups to access the best opportunities.
DeFi protocols have developed the most efficient money market, democratizing the access to debt. With no fiat currencies around, DeFi has built the perfect ecosystem around cryptocurrencies, from collateralization to interest payment, everything run smoothly almost commissions-less.

Without access to funding and debt, the entire DeFi ecosystem would be almost meaningless, these protocols represent the fuel of decentralization, and it's fundamental to understand and comprehend their functionalities.
The main protocols are Compound, Aave and MakerDAO, their services are slightly different from each other, but all three made the bankless lending and borrowing mechanism possible.

Borrowing volume from September 2020 to September 2021



SOURCE: TokenTerminal.com

Compound: It's an open-source money market based on Ethereum blockchain built by Compound Labs.
Basically, Compound lowers the friction between suppliers and borrowers, ensuring convenient APY (Annual Percentage Year) to liquidity suppliers and easing the access to debt for borrowers.
A question may rise: How much It is safe to lend money to an unknown individual without the control of a regulator?
The answer is contained in the smart contract itself that manage the service.
As soon as the borrower deposit the collateral into the system, a collateral ratio is provided, which is a measure to indicate the accessible funds in relation to the collateral deposited. If the value of the locked collateral goes down due to price variations such that the collateral ratio is now under the required level, a partial/total

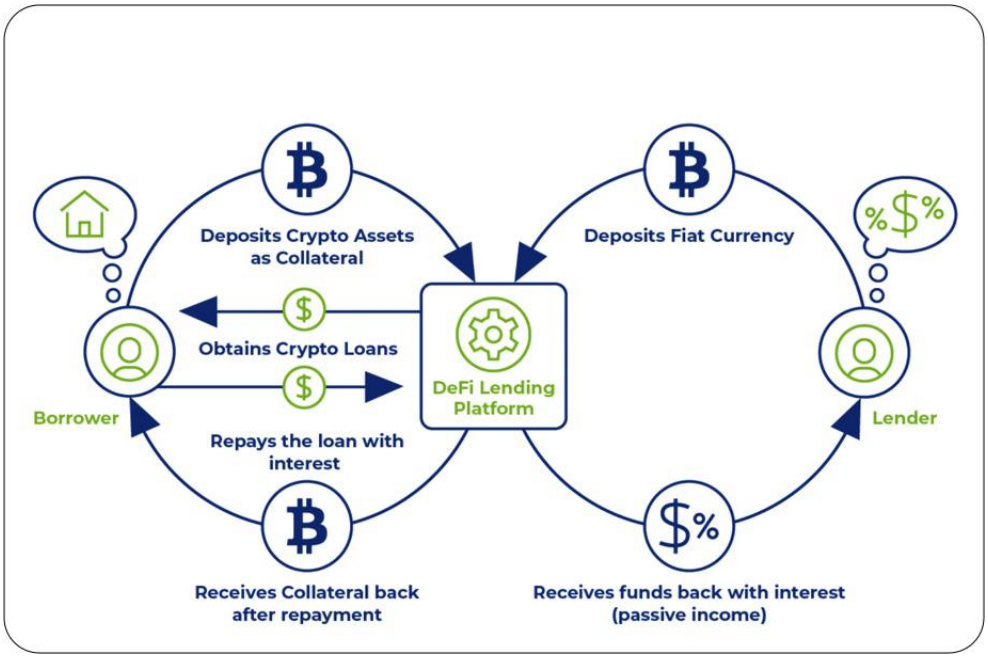
liquidation occurs. The liquidation feature is required to protect lenders against default risk.

MakerDAO: It's one of the oldest protocols, and, as explained before, Maker is also the stablecoin provider of DAI.
Unlike its competitor Compound, the Maker protocol allows its users to generate DAI by leveraging collateral assets. This is how Dai is entered into circulation and how users gain access to liquidity.
The smart contract which manages the entire operation is called Maker Vault and provide the same protection to lenders as Compound, with a collateral ratio.

Aave: on the surface, Aave is organized around the same concepts as the other two platforms. It works using liquidity pools and smart contract as usual. It's not user friendly as Compound but offers a couple more services.
Collateral swaps: borrowers can change their collateral with other asset, to prevent the possible devaluation of the collateral ratio.
Flash loans: borrowers can obtain loans without collateral, if they repay the loan and any interest in the same transaction. Basically, the funds are both borrowed and returned in the same moment. They are useful for who is looking for liquidity arbitrage opportunity. Flash loans can be considered a work in progress but up to July 2021 Aave had issued almost $4 billion in flash loans.

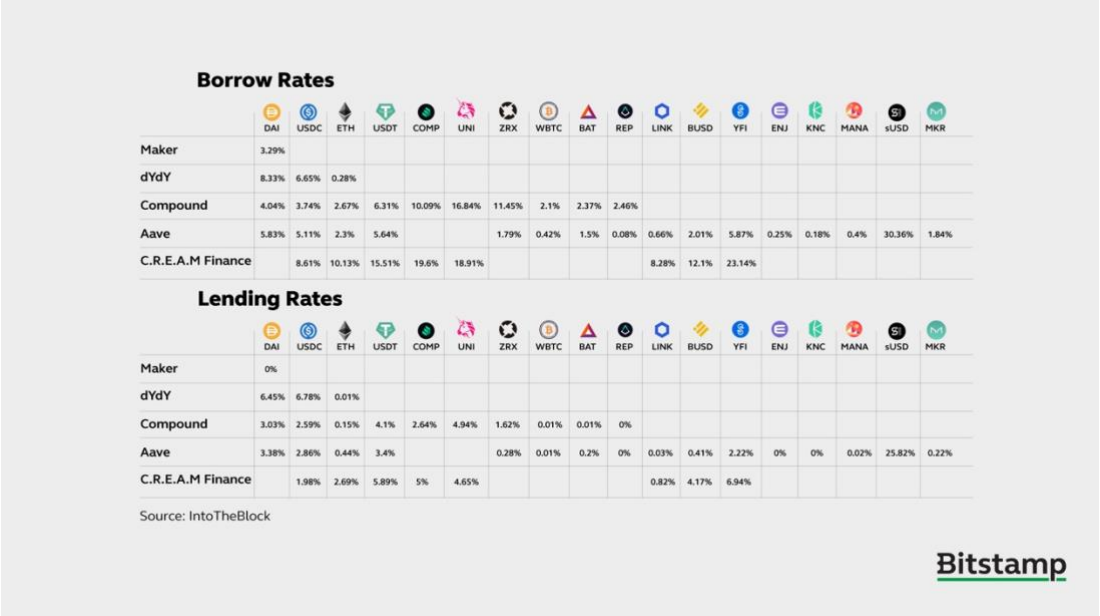
DeFi lending & borrowing protocols are probably the most appetible and useful tools in DeFi space, but they far from perfection.
In the traditional financial system, the decision to grant a loan or not is taken after a careful analysis of borrower's profile and data; at the moment the only one assurance in DeFi is overcollateralization, which cause a poor capital efficiency.
Also, DeFi is forced in the crypto niche, real asset collateral doesn't have a big place in decentralization yet. A big step has been taken, in 2021 Maker has introduced the possibility to use real estate asset as collateral in its platform.

How lending & borrowing works



SOURCE: yield.app

DeFi protocols and their rates



Borrow Rates

	DAI	USDC	ETH	USDT	COMP	UNI	ZRX	WBTC	BAT	REP	LINK	BUSD	YFI	ENJ	KNC	MANA	sUSD	MKR
Maker	3.29%																	
dYdY	8.33%	6.65%	0.28%															
Compound	4.04%	3.74%	2.67%	6.31%	10.09%	16.84%	11.45%	2.1%	2.37%	2.46%								
Aave	5.83%	5.11%	2.3%	5.64%			1.79%	0.42%	1.5%	0.08%	0.66%	2.01%	5.87%	0.25%	0.18%	0.4%	30.36%	1.84%
C.R.E.A.M Finance		8.61%	10.13%	15.51%	19.6%	18.91%					8.28%	12.1%	23.14%					

Lending Rates

	DAI	USDC	ETH	USDT	COMP	UNI	ZRX	WBTC	BAT	REP	LINK	BUSD	YFI	ENJ	KNC	MANA	sUSD	MKR
Maker	0%																	
dYdY	6.45%	6.78%	0.01%															
Compound	3.03%	2.59%	0.15%	4.1%	2.64%	4.94%	1.62%	0.01%	0.01%	0%								
Aave	3.38%	2.86%	0.44%	3.4%			0.28%	0.01%	0.2%	0%	0.03%	0.41%	2.22%	0%	0%	0.02%	25.82%	0.22%
C.R.E.A.M Finance		1.98%	2.69%	5.89%	5%	4.65%					0.82%	4.17%	6.94%					

Source: IntoTheBlock

Bitstamp

SOURCE:

3.4 Decentralized derivatives

A derivative is a type of financial contract whose value is defined by an underlying asset or groups of assets such as stocks, bonds, and other type of securities. The use-cases of derivatives are the speculation on the directional movement of an underlying asset and the hedge against volatility.

The most famous type of derivatives are options, futures, and swaps. Derivatives can be considered as leveraged assets, more risk, but also more possible returns.

In the last two years, the development of the DeFi ecosystem has seen also the inclusion of different decentralized derivative exchanges, such as Synthetix and dYdX.

Synthetix is a protocol which supports synthetic assets (Synths) on the Ethereum blockchain.

Synthetic assets are tokenized derivatives, they track the value of an underlying assets and offer the exposure to them without the need to actually hold them. They essentially allow investors to tokenize and trade with anything. With this protocol investors can easily trade anything on the blockchain. One of the main reasons why synthetic assets are becoming a preferred method of investing is because of the added security and traceability. While traditionally trading happens on centralized exchanges, with synthetic assets, all trades happen on the blockchain. This guarantees traders both their anonymity, and their security.

An example of Synths is sXAU (synthetic gold), the value of sXAU follow the price movements of gold.

There are also the counterparts, the Inverse Synthetic Asset, a derivative which tracks the inverse prime performance of an asset. A perfect example is iBTC (inverse Bitcoin).

Synthetic assets are so unique because they allowed users to be exposed to any real asset in a completely free and frictionless way, there's the possibility to switch any Synths at any moment, passing from Synthetic Gold to Synthetic Silver just with a couple of clicks, an operation that would have required a big amount of paper and time in the traditional financial system.

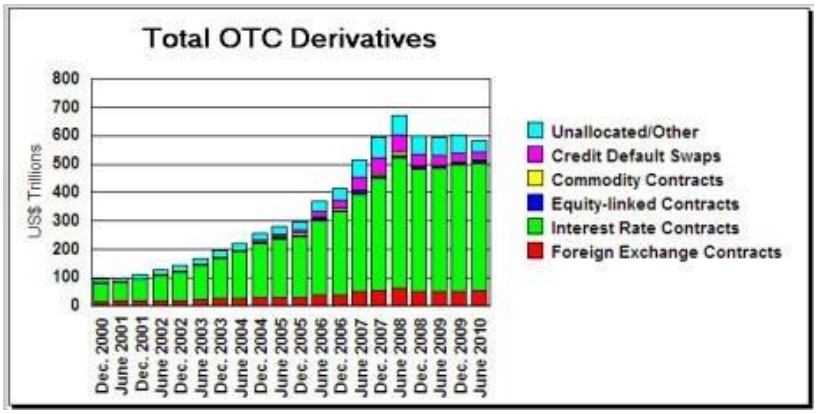
Another interesting aspect of decentralized derivatives are Index Synths.

The logic of Index Synths is the same of normal Synths, they exposed the user not to an underlying asset, but with a basket of asset. They are particularly useful in risk diversification because they consist in a wide range of products.

For example, the sDEFI Index Synth provide an exposure to the whole DeFi environment.

All these products are accessible through the Synthetix exchange, which employs liquidity pool to operate, the Synthetix dominance in the decentralized derivatives market is of almost 55%, with a total value locked of $1.88 billion. If we think that the traditional derivatives markets are estimated to involve up to $1 quadrillion, we realize that the space of growth of this decentralized sector is practically endless.

Traditional derivatives markets



SOURCE: siliconvalleywatcher.com

3.5 Decentralized insurances

Since its conception during the Renaissance, the insurance industry has accompanied every type of business.
Insurances help business and people to discharge low frequency risks, easing risk management.
Insurances strongly rely on two main assumptions:
Law of large numbers and risk pooling, as the number of exposure units (policyholders) increases, the probability of an actual loss shrinks.

"Suppose that a health insurance company discovers that five out of 150 people will suffer a serious and expensive injury during a given year. If the company insures only 10 or 25 people, it faces far greater risks than if it can ensure all 150 people. The company can be more confident that 150 policyholders will collectively pay sufficient premiums to cover the claims from five customers who suffer serious injuries." [1]

In a crypto driven ecosystem, where price volatility and insecurity related to the use of new technologies are the main entrance barriers for big and institutional investors, the need of insurances is remarkable.
The biggest insurance protocol is Nexus Mutual, with a total value locked of $510 billion, offers two types of covers:
Protocol covers, principally based on smart contracts malfunctions and bugs, and includes

- Oracle failures
- Governance attacks
- Protection for non-Ethereum smart contracts
- Protection for protocols across multi chains

[1] *Example from www.investopedia.com*

Custody covers, which are focused on risks of funds getting hacked or when the withdrawal is blocked. They also offer covers for deposits on CEXs such as Binance, Coinbase, Gemini and centralized lending & borrowing platforms such as Blockfi and Celcius. The coverage is priced using different criteria: the type of smart contract that requires coverage, the cover amount, the cover period, and the value staked by Risk Assessors against the smart contract.

Who is a Risk Assessor? A Risk Assessor is an individual who analyze the potential risks of a smart contract and stake value against it, assuring its security. He's incentivized by receiving earning rewards in Nexus Mutual token (NXM).

Let's suppose a user got an insurance cover on Nexus Mutual and one of the events which is included in the cover strikes. What does he need to do in order to access the refund?
The process of getting refunds after a covered event is called Claim Assessment. The user can send the claim at any time with a maximum of 2 claims per policy. The result of the claim is decided by members voting, to become member is required a stake of Nexus Mutual tokens (NXM).
To be eligible for a valid claim, users will have to prove that they have lost at least 20% of funds for Protocol covers, or at least 10% of funds for Custody covers.

4. RELATED TECHNOLOGIES

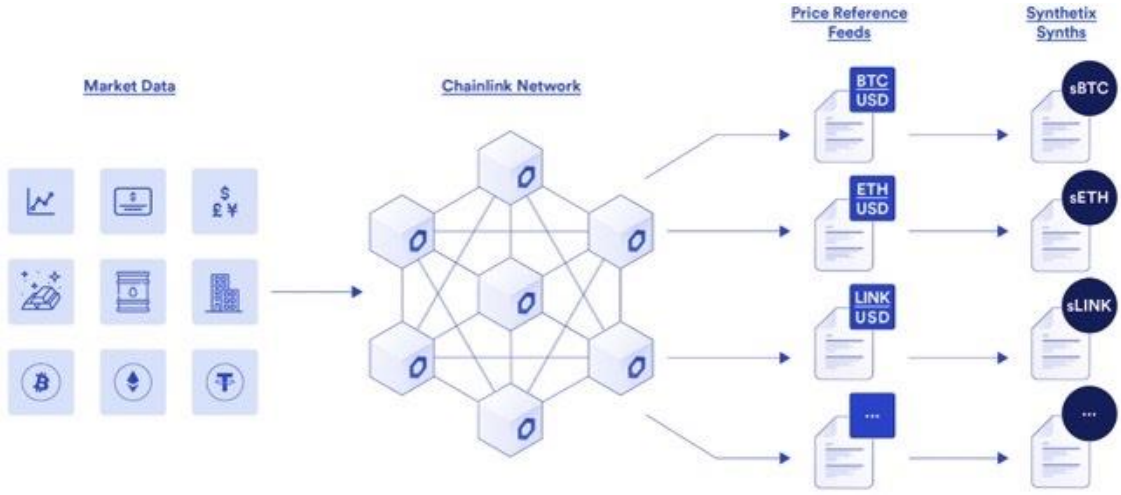
DeFi is the results of the relation between various technologies, some are the core of decentralization, and others are indispensable for the proper function of some protocols. With the birth of such complex ecosystem, new technologies have been developed to fulfil new needs.

4.1 Oracles

Oracles can be considered intermediaries, they feed the smart contract with off-chain data, which means that they help blockchain's protocols to reach external data.
The oracle act as a plug-in in the smart contract enabling it to access external data sources (inbound), and they also work in the opposite way, permitting smart contracts to send on chain data to external receivers (outbound).
These links between blockchains and off -chain data can be of two types:
Hardware oracles, for example any type of sensors, due to their physical nature, these types of oracles are not fit for a role in a decentralized world.
Software oracles are widely used in DeFi sectors such as stablecoins and decentralized derivatives.
One network can be considered the protagonist of oracle's technology, Chainlink.
Chainlink is an open-source technology which builds decentralized oracle networks.
The data delivered to smart contracts are the result of the aggregation of many data sources, the differentiation of sources is needed to maintain the decentralization principles. The Chainlink technology integrates with many different blockchains which requires oracles' services. Previous analyzed protocols use off-chain data provided by Chainlink.
MakerDAO (lending & borrowing protocol) utilizes oracles to determine the real values of assets supported in its platform. A median price of assets is determined combining price values from different data sources.

Synthetix uses Chainlink's oracle network to access information of real-world market price of the underlying assets of their Synths.

Chainlink role in Synthetix protocol



SOURCE: blog.synthetix.io

Chainlink is also collaborating with Google since 2019. It's using the Google Cloud's Big Query to access important weather data provided by the U.S National Oceanic and Atmospheric Administration (NOAA). These data are then fed to decentralized insurance protocols, which are going to use them to better price coverages, calculating the probabilities of disastrous climate events.

As for all new technologies, oracles are always a "work in progress" reaching every year a new level of efficiency. There are related risks such as hackers' attacks vulnerability, since oracles networks are outside any blockchains reality and consequently, also outside the consensus mechanism of such technology.

4.2 Bridges

Because of their structural design, blockchains are isolated, and due to this handicap, users of DeFi protocols are often locked in a single network, while the communication between different blockchains would be much more efficient.

Bridges resolve the interoperability problem, allowing the transfer of data, tokens, and even smart contract to between independent blockchains.

Bridges resolve scalability and efficiency problems; high transaction volume bridges enable users to drive out congestions from one blockchain to another.

For example, if gas fees on Ethereum are too high because of congestion, instead of paying such a large amount, an user could use a bridge to move its funds to a cheaper network, for example, Polkadot or Cardano. The bridge technology enables users and developer to combine the best aspects and characteristics of more networks.

Bridges are also fundamental tools for the correct functioning of sidechains.

A sidechain is a separate blockchain which runs parallel to the main one, with a child-parent relation. It has different consensus mechanism and enables the rise of different crypto branches and use cases.

The perfect examples of sidechains are the Polkadot parachains. They have all the main benefits of the Polkadot blockchain but also highly specialized functions.

It’s clear now that even if sidechains grow from the main blockchains, their communication requires bridges.

In the DeFi contest, bridges are an indispensable tool for the creation of dynamic and efficient ecosystems.

5. THE FUTURE OF DEFI

The TVL (Total Value Locked) in the recent years is skyrocketed and it's the main metrics to look at to understand and forecast the DeFi growth:

- 2018 TVL $275 million
- 2019 TVL $667 million
- 2020 TVL $15.7 billion
- 2021 TVL $82.33 billion (September 2021)

  SOURCE: defipulse.com

All the basics and opportunities made clear that DeFi is going to have a big spot into people's life in the future, but where is DeFi right now and where is it headed?

5.1 Institutional adoption

Mass adoption would not occur from day to night, it would require a slow and meticulous process that has already started. In the early years of cryptocurrencies fame, most of the big financial entities have openly criticized Bitcoin and the entire ecosystem, now, those exact same entities are the in the first line trying to take advantage of it. Goldman Sachs offers investments to digital asset class to his clients, BlackRock announced that they're trading digital assets, these are just the main examples of what is happening right now.

In 2021 Aave built a private pool for institutions, to allow them to have a first touch of the ecosystem before entering it.

The decentralized world came up at the eyes of the masses also through the help of big companies and big personalities.

Currently, the DeFi ecosystem is not safe and regulated enough to permit a total and comprehensive institutional adoption, but the network development has been parabolic since 2018 and it will not stop in the foreseeable future.

5.2 When NFTs meet DeFi

DeFi is an ecosystem that has almost infinite way to manage monetary assets, and with the possibility to build boundaryless relationships between users. Now let's imagine this reality merging with the concept of ownership and property of NFTs.

Both are the complement of each other, the result of this encounter has a perfect balance and thousands of possible applications.

A clear example is the always growing gaming industry, that it's currently really involved into the development of crypto games, a new frontier that has decentralization and property as core concepts.

Games where all the achievable objects are tradable NFTs on a secondary market or locked as collateral to obtain in game advantages. It's clear that such a complex and engaging ecosystem would rise the demand of such technologies to the point that their potential would be understood also by the average people. The perfect example is the game "Axie Infinity", an online game where all the creatures inside it are NFTs, it has recently reached a total of $1,6 billion in game sales. Inside the game you can gain the ownership of the creatures through a minting process (launching process) but due to the enormous demand and the limited supply, it's often impossible to get the rarest one (all the creatures have different rarities traits). If you've been lucky enough to get one, you have the possibilities to lend it to other people in exchange of an interest rate.

The users have now the possibility to build their digital lives around these technologies, the so called Metaverse can be considered as an alternative reality, built upon a blockchain, where all the transactions occur through cryptocurrencies, and the certifications of property rely on NFTs. People can buy pieces of virtual lands of famous virtual worlds such as Decentraland and SandBox, with the possibilities to build communities and societies around it.

The enormous utility offered by DeFi and NFTs will definitely be the leading force of mass adoption in the foreseeable future.

5.3 Incoming regulations

When we think about the Internet's impact on the economic world ad society, we notice that the only reason why internet didn't completely disrupt the banking sector, like it did it with every other industry, it's because of regulations.

Regulations can be seen in two different ways, like a brake to the disruptive rise of the DeFi ecosystem or as proof of legitimacy and security. The reality is constituted by the match of both situations. Undoubtedly, incoming regulations would constitute a slow down for the numerous realities in DeFi, but they would set at least minimum standard requirements, in particular to subjects such as consumer protections, which is one of the main reasons behind the reluctance of big institutional investments.

The key success factor of the regulatory transition is a balanced approach, too strict regulations could severely damage DeFi adoptions and promote adverse reactions.

Any type of regulations will not be immediate, this is caused by different factors.

First, the fragmented nature of DeFi, made clear by the definition of LEGOs money, significantly slow down any reglementary approach. Second, because of the decentralized structure, regulator struggle to identify responsibilities.

The first realities to have been hit are the centralized one, for example, the SEC (Security and Exchange Commission) threatened to sue Coinbase over the launch of its lending platform where users could have been able to land their stablecoins in exchange of interests.

CONCLUSION

DeFi undoubtedly marked a turning point in both technological and financial world. Some of the brightest minds of the planet, combined with the need to make a financial and social change, have brought to life one of the most flourished and complex ecosystem ever seen. DeFi, and all the technologies under it, are giving to people full control and ownership of their asset, with the possibility to live off them, leveraging to the fullest the meaning of property. Smart contracts and protocols are allowing people to monetize things that they have never been able to monetize before, without any regulator's restrictions and biases.

DeFi is not under a government control, it is not under any political lobby, and it's not even under any central bank.

But it has geopolitical implications and interests, for example, with the birth of internet, the USA built an amazing infrastructure, they have built the Silicon Valley, and they have led the way of the internet revolution. The USA geopolitical power it's an effect of that revolution. Who is going to lead the development and growth of DeFi? Apart from regulations, countries and companies are definitely looking carefully to the new decentralization's trends, making sure to don't miss another epochal revolution.

It's important to remember that DeFi is built for people, giving to everyone the possibility to approach any financial services, from lending & borrowing, to derivatives and insurances.

According to a document released by the World Bank in 2018, there are almost 1.8 billion people without access to financial services because of lack of infrastructures, political instability, and conflicts. DeFi offers a reasonable solution, everyone with a smartphone and an internet connection has now the possibility to access basics financial services. It's important to don't forget that this is the main mission of the DeFi reality, allow people to take control of their assets, properties, and lives.

Bibliography

Nicola Attico
Blockchain: guida all'ecosistema, 2018

CoinGecko
How to DeFi, 2020

CoinGecko
How to DeFi advanced, 2021

Saravanan Krishnan, S. Balaji, Valentina E. Balas, Y. Harold Robinson, Raghvendra Kumar, E. Golden Julie
Handbook of research on blockchain technology, 2020

Sitography

www.coinmarketcap.com
www.coingecko.com
www.investopedia.com
www.cointelegraph.com
www.coindesk.com
www.washingtonpost.com
www.forbes.com

Data Sources

www.defipulse.com