DeFi and Start-Ups: Revolution in Finance

Juan Piñeiro-Chousa, Ángeles López Cabarcos, and Isaac González

1 The Concept: Internet of Value

Transfer value over digital networks without a middleman is the main idea behind the expression ‘the internet of value’. This also refers to the revolution that the internet has generated regarding information interchange and the potential revolution regarding value interchange.

This chapter will describe the key concepts that open new possibilities for finance and startups.

1.1 Decentralization

Removing the intermediary with open and trustworthy technology is probably the most crucial concept recognized in the cryptocurrency movement. The goal of Bitcoin was to create a currency without the need for central banks and commercial banks; in other words, the aim was the decentralization of digital currencies. Thus, Bitcoin started the movement that other projects have followed by applying this idea to new areas with different perspectives.

1.2 Permissionless

Physical money allows two parties to make a deal without asking for permission from a third party. Consider this an example: Person A exchanges $10 for 8 € with Person B. Nevertheless, digital money, as we know, is not so straightforward, especially in an international environment and with different currencies. First, both

J. Piñeiro-Chousa (✉) · Á. L. Cabarcos · I. González
Santiago de Compostela University, Santiago de Compostela, Spain
e-mail: j.pineiro@usc.es; angeles.lopez.cabarcos@usc.es; isaacjose.gonzalez.lopez@usc.gal

C. Lassala, S. Ribeiro-Navarrete (eds.), *Financing Startups*, Future of Business and Finance, https://doi.org/10.1007/978-3-030-94058-4_10

persons would need to ask a bank for a digital account, which has several requirements, depending on the country. Then, there are several steps that need to be completed, such as international bank transfer slips and currency exchanges. In the best-case scenario, there is one-third party that helps make the exchange possible; in the worst-case scenario, there are several parties and many operations that help make it possible. In addition, one party can deny the operation for any reason, and then the transaction cannot take place. Decentralization also implies that no one party has the power to concede or deny access to the system.

1.3 'Don't Trust, Verify'!

If anyone can participate and there are no middlemen, then the only way to trust the system is by using glass walls. The open-source movement is critical in the software industry; it brings about transparency in publishing the code so that anyone, primarily specialists, can see how it works. In addition, when protocols need transparency, a committee releases documentation that describes the rules, details and anything related to the protocol. In this way, anyone can implement, use or interact with the protocol. Internet technology establishes an open protocol framework. The last requirement for trust is publicly available data, which collides with privacy. Most blockchains use anonymity to solve this matter; thus, everything is public, but there are no names, only account numbers.

In summary, with open-source, open protocols and anonymity, no one must trust technology or other parties; it is possible to verify everything. This idea has been condensed in the famous phrase in the crypto world: 'Don't trust, verify'!

2 The Technology: Blockchain and Smart Contracts

Technology that allows decentralized, permissionless and verifiable digital systems is a very impressive advancement. The turning point in history was the publication of the paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' by Satoshi Nakamoto and the development of the subsequent open-source program. However, the technology came long before that, and the improvements were countless, which makes this one of the most significant new industries worldwide. This chapter will describe the key concepts and central ideas of this technology rather than following its history. Presenting the base technology that decentralized finance uses is the goal of this chapter.

2.1 Distributed Ledger Technologies

A digital ledger is essentially a database that lists the transactions between accounts and the current balance of those accounts. All modern banks have digital ledgers implemented on databases with high levels of security. Since the bank owns its ledger, the bank could change it; however, regulations, laws, and central banks monitor the behaviour of banks to prevent such behaviour. This scheme works very well if the top organization does its duty. However, if the top organization is corrupt, the whole system is compromised. Is there any alternative to this system?

Distributed ledger technologies (DLTs) are digital implementations of ledgers without a single owner (Romero-Ugarte, 2018). Instead of the traditional approach with one person or organization being in charge of the database, DLTs use cryptographic technology to run the database distributed in several nodes.

To align incentives, the typical way to run a DLT is to ask for fees from users to settle a transaction (example: Account A sent $10 to account B plus a $0.05 fee) and distribute that fee over the nodes to help to keep the DLT up and running. On the other hand, if a node engages in malicious behaviours such as trying to settle incorrect transactions or not helping to run the DLT, the node can be punished.

In this way, there are rules to maintain a digital ledger in which nobody can change the state of the database unless it controls more than 51% of the nodes to settle fake transactions. Thus, there is a broad decentralization of nodes and a good balance of incentives and punishments.

2.2 Blockchain

A blockchain is a concrete implementation of distributed ledger technology (Yaga et al., 2019). Therefore, it is similar to a database of transactions without an administrator.

The transactions that occur during a specific time frame are packeted in a block. In Bitcoin, for example these blocks have a duration of approximately 10 min. In real time, all the transactions go to the present block. When the block time is over, the block is closed, and a new block is opened for the transactions that occur in the next 10 min. Blocks can be compared to pages of a ledger book, and transactions can be seen as its lines.

To assure that blocks are immutable, each block stores a hash code of the precedent block, thereby creating a chain of blocks. In this way, if any node wants to maliciously change a settled transaction, it should change the block of the transaction, which will change the hash of the following block, which will thus change the hash of the next block and so on until the present block. Chaining the blocks in this way makes it exponentially difficult to change past transactions.

There are other implementations of the DLT, such as Hashgraph, which is led by the Hedera Hashgraph project. However, the large majority of cryptocurrencies are created on blockchains.

2.3 Consensus: PoW vs. PoS

The consensus mechanism is seen as the process of reaching an agreement on the exact form of the block (Bach et al., 2018). Since many nodes handle transactions, it is possible to have different blocks without bad intentions; additionally, malicious nodes could have untrue blocks. Therefore, when the block time ends and must be settled, all the nodes must agree on the actual block and settle it; that is the consensus. The alignment of incentives is the key to reaching the consensus and the good health of the blockchain. If the node collaborates, it will be rewarded; however, if the node acts maliciously, it will be punished. There are two main ways to do this, namely proof of work (PoW) or proof of stake (PoS).

In PoW, nodes must pay upfront for a costly computational effort (a tremendous amount of calculus). If they act maliciously, it is effortless to catch them because the block will be very different from the rest of the nodes. Punishment, not reward, is what awaits the effort made. If they collaborate with the network, then the network will reward the nodes using a random algorithm so that the reward will eventually occur. Nodes in PoW are called miners. Since computational work is very intensive in electricity and bitcoin mining is very profitable, miners use a significant share of world electricity consumption.

In PoS, nodes must deposit (stake) several tokens. If they act maliciously, then they lose part or all the tokens at stake; collaborating with the network means a reward for them. There are many variations of the PoS algorithm, such as delegated (DPos), bonded (BPoS), and hybrid (HPoS) algorithms. Indeed, there are many variations in the staked amount required, the rewards, and other details. Nodes in PoS are called validators, and they are much less intensive in electricity consumption. There are alternative consensus algorithms such as proof of authority, proof of location, proof of history, proof of burn, and more. Additionally, they can be hybrid solutions. However, all proofs have in common the necessity of reaching consensus in a decentralized system. These are ways to resolve the Byzantine general's problem that was proposed in 1982 as a logical dilemma.

The rewards received by miners and validators come from transaction fees collected in the blocks they help settle and, in some cases, newly minted tokens. Each blockchain defines the consensus mechanism in open-source code that anybody can check and in a more human-readable documents called white papers.

2.4 Smart Contract

A smart contract is an agreement that is made in code and executed in a blockchain. In this way, the two parties do not need to trust each other or a third party because the code is open-source, and the execution is unstoppable.

From arithmetic and computational perspectives, a ledger has a very restricted set of arithmetic operations. For example when Account A sends $10 to Account B, the operations involved are Account A balance minus ten and Account B balance plus ten. Ethereum and other blockchains were created to expand the operations allowed on a DLT to all the operations and structures of a computer code.

Nick Szabo coined the term smart contract, and Etherum was the first successful blockchain to implement the concept. The term came from the goal of providing a way to transform agreements into code executed on a neutral infrastructure.

However, the process should not hide its real essence, which is a computer code that runs over the nodes of a blockchain.

Before the arrival of smart contracts, the agreements should rely upon the trust of two parties or a trusted third party to assure that the agreement is fulfilled. For example if person A bets $10 with person B on the victory of the Lakers in their next match, either they trust each other, or they need a third party they both trust. With a smart contract, the agreement can be transformed into code and executed in a blockchain. Both conditions must be true; otherwise, if the computer in which the code is executed belongs to one party, if that party loses, the party could turn off the computer and thus make the code not be executed and the agreement not be fulfilled. Thus, smart contracts and blockchains remove the need to trust the other party in any agreement.

Example 10.1

```
send(A,BET,10) # Send 10 dollars From A account to BET account
send(B,BET,10) # Send 10 dollars From B account to BET account
if (lakers_win == true)
 send(BET,A,20) # If lakers win send 20 dollars to A
else
 send(BET,B,20) # If lakers not win send 20 dollars to B
```

2.5 Tokens

Some people use Bitcoin (capital B) as the name of the blockchain, bitcoin (lowercase b) for the cryptocurrency and BTC as the ticker. When Ethereum was created, Ethereum was used for the blockchain, Ether was used for the cryptocurrency, and ETH was used as the ticker. Until that moment, each blockchain had its own cryptocurrency. However, when Ethereum implemented the ERC20 feature, it allowed us to easily create new cryptocurrencies over the Ethereum blockchain, which are called tokens. Since their establishment, the creation of tokens has skyrocketed. Some authors use cryptocurrency for those running on their own blockchain and tokens for those running on other blockchains; however, in the literature, it is very common to see tokens as being synonymous with cryptocurrency.

Oxford dictionary defines a token as ‘a round piece of metal or plastic used instead of money to operate some machines or as a form of payment’; we can apply this idea to the decentralized digital space. Cryptotokens, or simply tokens, bring an important novelty; i.e. everything is verifiable because it is created and traded on the blockchain.

3 Decentralized Finance

Decentralized finance, or DeFi, is the replication of financial services with smart contracts over blockchains, following the main features of crypto, i.e. the removal of intermediaries and permissionless use. Another vital feature of DeFi is composability. Since anybody can access any service without permission because of the open protocols, it is possible to create new services that use, improve or complement several services. This property is behind the famous phrase: DeFi functions as money Legos.

Cryptocurrencies are in essence a financial product. They are tradeable, they represent a digital asset, and they function as a digital form of money (Baur et al., 2018). In addition, of course, they are decentralized. Therefore, why is decentralized finance a subcategory in crypto? In short, DeFi tends to decentralize financial services prior to 2020 were in centralized crypto exchanges or traditional banks. Some authors share this financial services view (Gudgeon et al., 2020; Schär, 2020), while others have a wider categorization of DeFi (Chen & Bellavitis, 2020).

In the next sections, we will describe most of the DeFi categories and compare the centralized service with the decentralized version. It is important to note that this topic is very recent and is constantly changing. To support the definitions, we will refer to real projects that led the category at the time of the writing of this article. To describe the projects, we use whitepapers and official documentation, which is linked at the end of the chapter. This categorization is debatable and fuzzy; in fact, most sources have different categorizations, and some projects could be placed in several categories. However, our aim is to be educational in describing the roots but not formal in regard to categorization.

3.1 Stablecoins

Most cryptocurrencies are free trading, which means that they are priced by the market. In a very new technology with extremely fast adoption, the volatility is huge (Yin et al., 2021; López-Cabarcos et al., 2021), as shown in Fig. 1. The solution is the creation of a token that represents the price of an off-chain coin, which in most cases is linked to US dollars (USDs). This is called a stablecoin because its price is pegged to a real currency (Ante et al., 2021). Stablecoins are very useful when avoiding volatility and as a haven in crypto downturns. Therefore, they are a key part of the cryptocurrency ecosystem.

The first successful stable coin was USD Tether (USDT). As Fig. 2 shows, the price is most of the time very close to 1$. Tether is a company that mints one USDT token on-chain backed by one USD off-chain; in case of a reduction in supply, then they burn USDT tokens in the same amount of USD that they withdrew. Even on a blockchain, this is considered a centralized way to create a stablecoin because USDT users must trust in Tether's behaviour, audit behaviour or bank behaviour. Indeed, there have been concerns that USDT could not be fully backed. These concerns have attracted other players to create their own stablecoins, such as USDC (Coinbase), BUSD (Binance), HUSD (Huoby) and others.

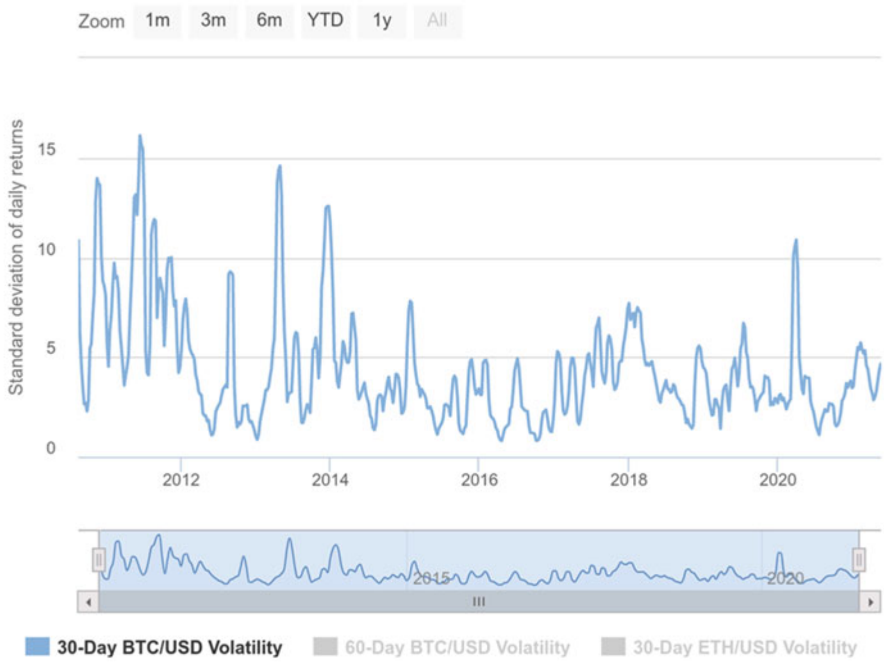


Fig. 1 BTC/USD volatility. Source: coinmarkecap.com

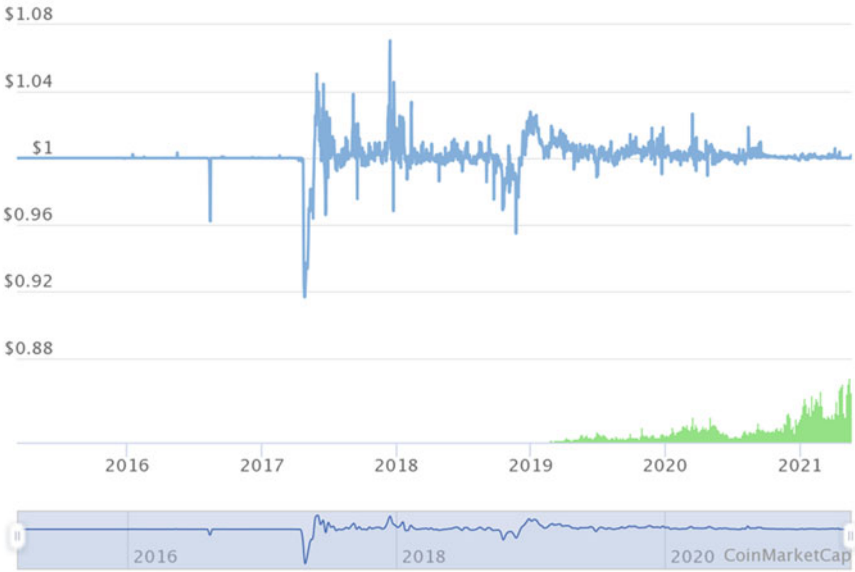


Fig. 2 USDT price chart. Source: coinmarkecap.com

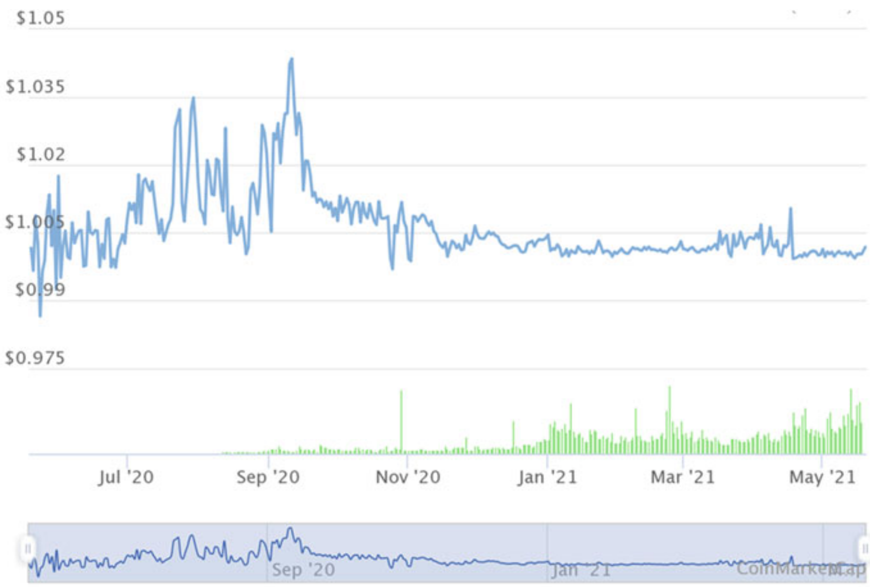


Fig. 3 DAI price chart. Source: coinmarkecap.com

Maker is a crypto project that creates a decentralized fully on-chain stablecoin called DAI, where 1 DAI is equal to 1 USD. Anybody can borrow DAIs by depositing ETH (or other cryptocurrencies) as collateral, such as a mortgage. The user can define the collateralization ratio starting at 150%. For example if the user chooses 200%, then he or she deposits 0.2 ETH ($200 at that moment) and he or she then receives 100 DAI. Overcollateralization is important to prevent the price falling of the deposit because if the price of the deposit falls under the collateralization ratio, then the position is automatically liquidated. For example if the 0.2 ETH that was deposited is now worth $120 under the 150% liquidation ratio, then the user loses the ETH and keeps the 100 DAI. This is called a collateral debt position (CDP) The Fig. 3 shows DAI is very close to 1$, particularly in recent times.

Ampleforth (AMPL) is another stablecoin that uses a less effective strategy. Instead of CDPs, Ampleforth has a smart contract that mints new AMPL when the price is higher than expected and burns AMPL when the price is less than expected. This idea is based more on supply reducing prices and less on supply increasing prices. Ampleforth is pegged to USD plus the Consumer Price Index to avoid inflation. As shown in the Fig. 4, the stability of the token remains questionable, but DAI or even USDT also had these stability problems in the beginning.

3.2 Lending and Borrowing

Lending and borrowing are key services in any financial system. Traditionally, banks offer loans, credits and mortgages to clients. Based on risk studies or backed

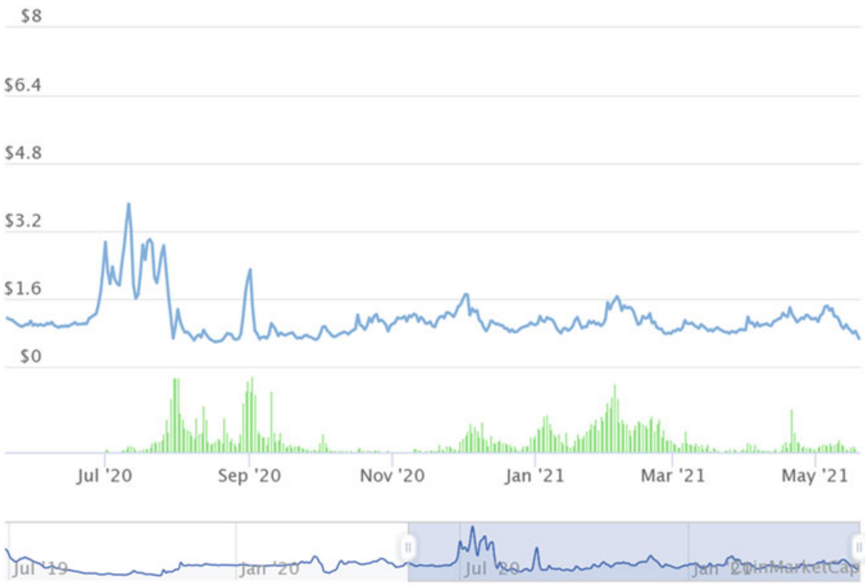


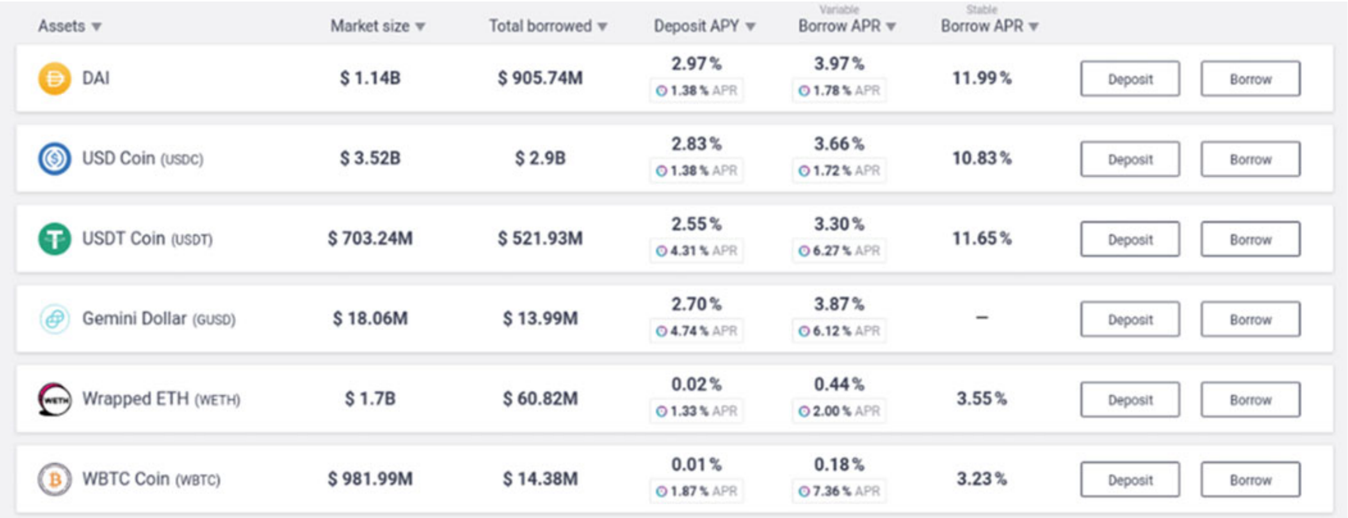
Fig. 4 Ampleforth price chart. Source: coinmarkecap.com

by collateral such as a real estate, the interest rate is adjusted to the situation. On the other hand, savers deposit money in banks and receive a yield. The bank acts as a central authority that makes decisions, and clients must trust these operations.

Of course, on a blockchain, two persons can agree on a relationship between the lender and borrower in their own terms. Indeed, there are centralized services that offer lending (deposit) and borrowing services (such as Nexo, Cello, Blockfi etc.). Additionally, centralized exchanges offer this kind of service. However, in this way, the client should trust the other party. This is centralized finance over blockchain.

When creating a lending and borrowing system in a decentralized way, the challenge is to create a decision-free mechanism of on-chain assets. The goal is to create a smart contract that allows users to lend and borrow without human intervention, such as risk studies. The assets must be on-chain, such as cryptocurrencies or nonfungible tokens. The problem with off-chain assets is the impossibility of assuring that they are transferred between the lender and borrower, as defined in the agreement. Therefore, to borrow one cryptocurrency, the user must deposit a collateral. Protocols like Aave or Compound are the actual leaders of this category.

The previous Fig. 5 is a screen capture from Aave, which shows for each token the market size (total deposits), the total borrowed, the annual percentage yield (APY) earned by depositors, and the annual percentage ratio (APR) borrowers pay in a fixed or variable way. The APR and APY depend on the market. If there are too many deposits and fee borrowers, such as WETH or WBTC, as seen in the image, then the APR/APY are very low; however, if the opposite is true, such as DAI, then the APR/APY are higher. The borrower must deposit a collateral to guarantee that it will return the principal plus interest. A typical use case is offering as a collateral a



Assets ▼	Market size ▼	Total borrowed ▼	Deposit APY ▼	Variable Borrow APR ▼	Stable Borrow APR ▼		
DAI	$ 1.14B	$ 905.74M	2.97 % 1.38 % APR	3.97 % 1.78 % APR	11.99 %	Deposit	Borrow
USD Coin (USDC)	$ 3.52B	$ 2.9B	2.83 % 1.38 % APR	3.66 % 1.72 % APR	10.83 %	Deposit	Borrow
USDT Coin (USDT)	$ 703.24M	$ 521.93M	2.55 % 4.31 % APR	3.30 % 6.27 % APR	11.65 %	Deposit	Borrow
Gemini Dollar (GUSD)	$ 18.06M	$ 13.99M	2.70 % 4.74 % APR	3.87 % 6.12 % APR	–	Deposit	Borrow
Wrapped ETH (WETH)	$ 1.7B	$ 60.82M	0.02 % 1.33 % APR	0.44 % 2.00 % APR	3.55 %	Deposit	Borrow
WBTC Coin (WBTC)	$ 981.99M	$ 14.38M	0.01 % 1.87 % APR	0.18 % 7.36 % APR	3.23 %	Deposit	Borrow

Fig. 5 Screenshot of Aave user interface

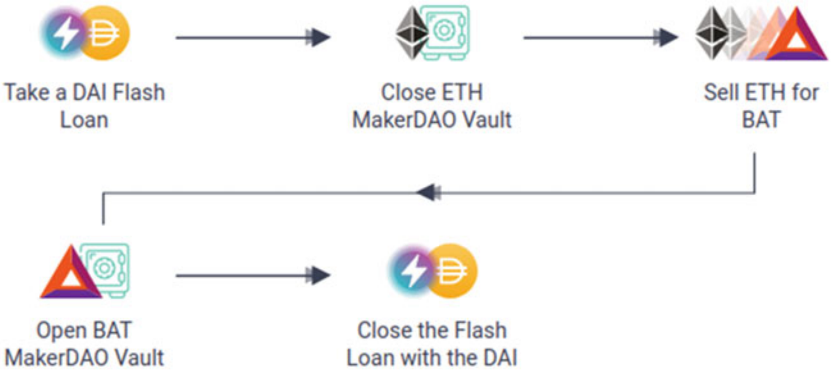


Fig. 6 Flash Loan use case: Collateral swap of a MakerDAO Vault. Source: Aave documentation

cryptocurrency that the user thinks is undervaluated and receiving a loan in the form of a stablecoin, while not losing the cryptocurrency's rise in value.

Flash loans are a very specific loan in crypto. They are loans that are asked for and returned in the same smart contract. This is similar to asking a bank for a loan, using the money inside the building for trade in a very short period of time and then returning the money to the bank. The use case of flash loans is mainly for price arbitrage. For example if the same asset has a tiny different price in two different platforms, any expert could create a smart contract to ask for a huge amount of money to buy the asset in one platform and sell it on another. Fig. 6 is another use case in which a flash loan allows to close an ETH MakerDAO collateral debt position and create a new one in other cryptocurrency and then return de flash loan. The risk of these operations is very low because the smart contract is either fully executed (including asking for and returning the loan) or is not executed at all. In addition, they are very short-term loans (minutes). Therefore, fast and secure loans mean tiny interests with no collateral. Flash loans add huge liquidity to the system, which makes possible arbitrages that balance the whole DeFi ecosystem. Additionally, these loans can be used to stress and even hack some protocols (Qin et al., 2020), which makes them safer in the long run.

3.3 Decentralized Exchanges

The goal of centralized exchanges (CEXes) is to provide a way to trade and custody currencies and cryptocurrencies. Additionally, CEXes can offer other services, such as deposit yields, derivatives, credit cards and more. The problem with that perspective is that people must trust the company behind the exchange. Mt. Gox was the leader exchange in approximately 2014; however, the company was hacked and lost all of its funds, which totalled approximately 850,000 BTC ($450 million at the time, $42 billion at the time of writing). The critical risk is the custody of the funds, which crypto users can handle by themselves with a software called a wallet and a password. Therefore, the difficulty of fully decentralizing exchanges is the trading service.

A decentralized exchange (DEX) provides a way to trade cryptocurrencies (Fig. 7.b shows the interface to make a trade, also called swap) in a peer-to-peer manner using smart contracts. In addition, it aims to decrease default or scam risks, add privacy (avoiding the 'know your customer policy' that CEXes have), reduce the arbitrariness of the service conditions, and offer full transparency.

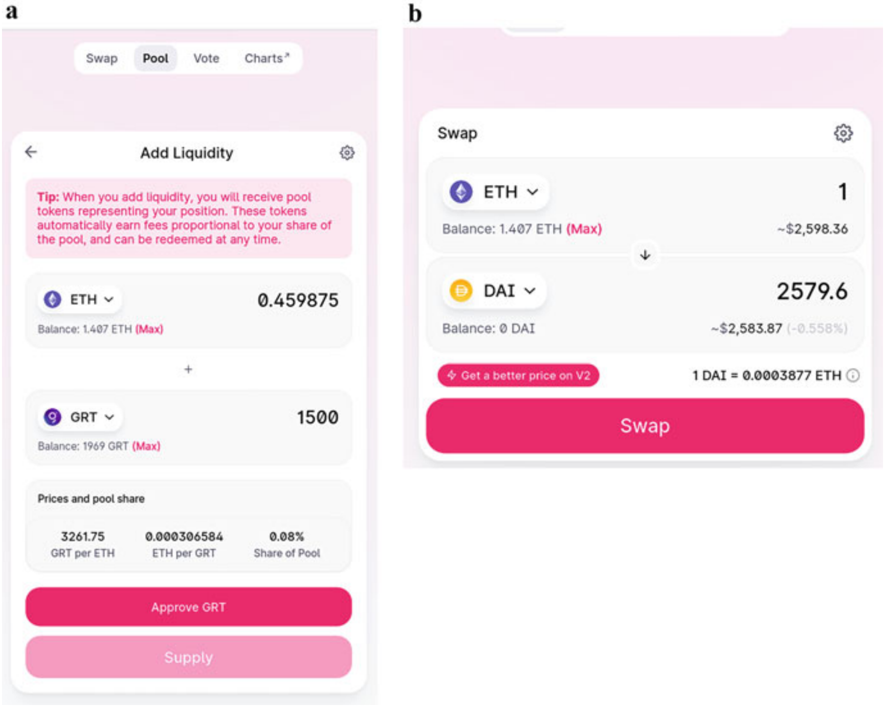
Of course, two parties can trade cryptocurrencies without a DEX, but a DEX offers the possibility to trade most cryptocurrencies at any time. Most DEXes use a form of automated market maker (AMM) (Wang, 2020) such that if one user wants to trade token A for token B, then that can be done because the DEX has a liquidity pool that contains those two tokens. The liquidity pool is filled with the deposits of many users (fig. 7.a shows the interface to provide liquidity to a pair of tokens). The trading user pays a fee for the trade, and the user that deposits tokens to the pool earns a proportional part of the total fees of the pool. The Fig. 8 below represent this process. For example in Uniswap, that fee is 0.3%; the deposits (total value lock) at the time of writing totalled $5 billion.

When a user provides liquidity with a pair of tokens (Fig. 7.a), the DEX gives back a receipt for the deposit. That receipt is in the form of an amount token, which are called liquidity provider tokens or simply LP tokens. LP tokens are a regular token, which means that they can be traded and used on the blockchain. At some point, some DEXes decided to incentivize people by giving rewards for specific pairs of tokens. The way to earn the reward is to stake the LP tokens after the deposit of that pair. This is called yield farming or just farming; it is a way to earn new tokens by simply staking some tokens on some specific DEXes.

3.4 Asset Management

The arrival of yield farming and a competition to attract liquidity providers to new platforms and their tokens brings about a new need, i.e. what would be the best way to stake the funds? Yearn Finance was created with that issue in mind. On the one hand, liquidity providers want to maximize their yield. On the other hand, experts propose strategies to maximize the yield earning fees if the strategy works well. In the middle is Yearn Finance; the platform was made with smart contracts to offer this possibility.

The Alpha Homora project brings about the possibility to earn yields with leverage. The combination of DeFi use cases such as farming and lending are good examples of how innovative this area can be based on openness and permissionlessness.



Tip: When you add liquidity, you will receive pool tokens representing your position. These tokens automatically earn fees proportional to your share of the pool, and can be redeemed at any time.

Fig. 7 (**a**) Screen capture of the interface to supply liquidity to a pool. (**b**) Uniswap interface for the traders

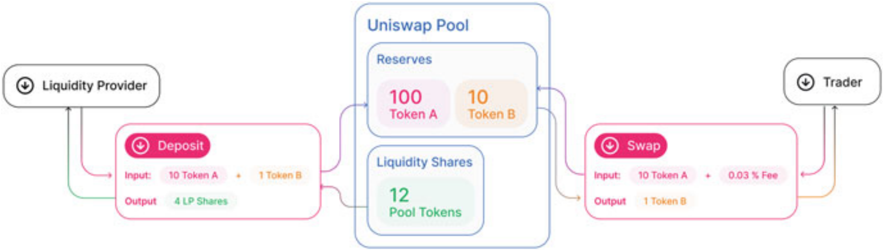


Fig. 8 Uniswap scheme of Uniswap pool, liquidity providers and traders. Source: Uniswap documentation

3.5 Funds

In traditional finance, funds are pools of money that have a specific purpose. For example a mutual fund is a pool made of investments by individuals managed by experts. They allocate funds to the assets they decide on according to the description of the fund. Another example is an ETF (exchange traded fund); in this case, instead of experts deciding on the investment, a basket of assets is made following the basket of assets in an index such as the S&P or Nasdaq to ensure that the fund follows the price of the index. An ETF can also follow the price of the basket of stocks from a category such as US small caps or European large caps, with defined the rules of picking the stocks.

The DeFi Pulse Index (DPI) is a token made with Set Protocol to represent the top DeFi protocols in Ethereum. It is like a DeFi ETF. It has clear rules that are coded in a smart contract to determine which assets to choose, and it weighs each asset depending on the capitalization. Each month, the tokens that compose the DPI are rebalanced following the rules. Set Protocol offers the possibility of anybody creating a basket of tokens similar to that of the DPI.

Enzyme Finance (formerly Melon) is an on-chain asset management protocol that enables anyone to set up and manage an on-chain fund or to invest in the funds. Enzyme, like Set Protocol, allows managers to create automatic strategies; however, unlike Set Protocol, Enzyme also allows manual decisions about the fund, thereby making the protocol closer to mutual funds than ETFs. The important part in both cases and in this category is that assets are staked on the protocol; thus, funds are fully backed. Indeed, managers can manage but cannot withdrawal to their own account during management because the funds are locked in the smart contract of the platform. Additionally, every action is traceable and public on the Ethereum blockchain.

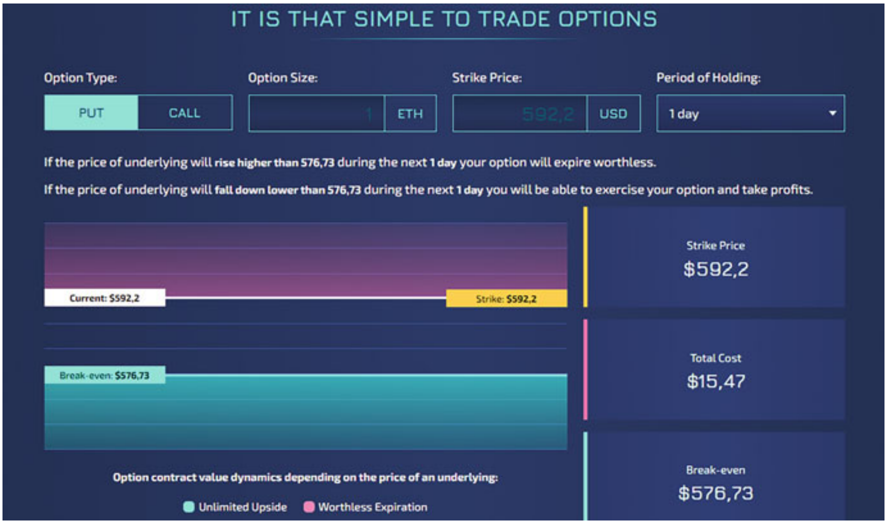
3.6 Derivatives

A derivative is a contract whose value is derived from another underlying asset (commodity, currency, stock, index, bond etc.). Futures, options and swaps are some derivatives with very different use cases. Derivatives are very risky instruments that are mainly used to hedge or speculate.

Centralized exchanges provide derivatives in a centralized manner. Some derivatives need orderbooks that act extremely fast to handle orders and price variations. At this moment, most blockchains cannot offer this service at a reasonable speed. Therefore, either derivatives are not critically time-dependent, or the protocol uses a less decentralized strategy for orderbooks, which is usually a second layer or a parallel chain.

Hegic is an example of the first case. It offers an on-chain options trading protocol, which allows users to either buy ETH calls and place options as an individual holder (buyer) or sell ETH calls and place options as a liquidity provider (Fig. 9).

DYdX is an example of the second case. It is a DEX like Uniswap, but it also offers leverage trading (lending-borrowing) and perpetuals (similar to futures) on layer 2. There are many protocols that implement options in very different manners (Fig. 10).



IT IS THAT SIMPLE TO TRADE OPTIONS

Option Type: PUT CALL

Option Size: 1 ETH

Strike Price: 592,2 USD

Period of Holding: 1 day

If the price of underlying will **rise higher than 576,73** during the next **1 day** your option will expire worthless.

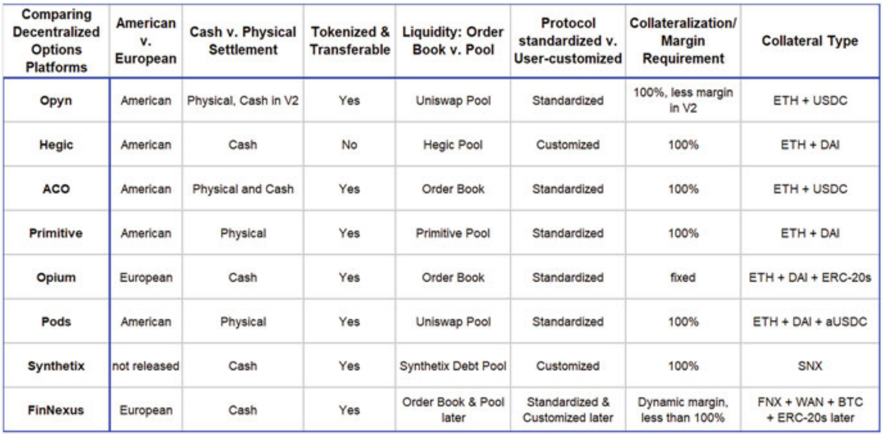
If the price of underlying will **fall down lower than 576,73** during the next **1 day** you will be able to exercise your option and take profits.

Strike Price $592,2

Total Cost $15,47

Break-even $576,73

Fig. 9 Screen capture of the Hegic interface

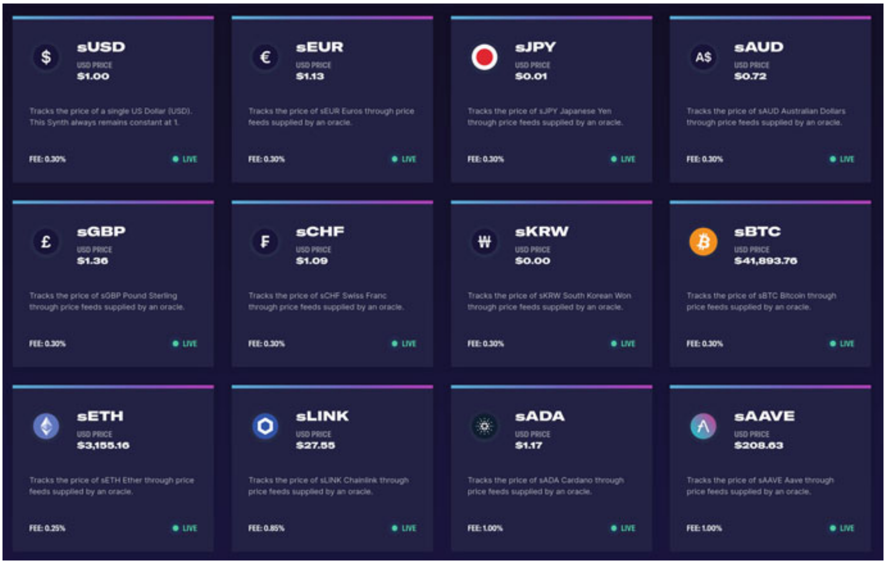


Comparing Decentralized Options Platforms	American v. European	Cash v. Physical Settlement	Tokenized & Transferable	Liquidity: Order Book v. Pool	Protocol standardized v. User-customized	Collateralization/ Margin Requirement	Collateral Type
Opyn	American	Physical, Cash in V2	Yes	Uniswap Pool	Standardized	100%, less margin in V2	ETH + USDC
Hegic	American	Cash	No	Hegic Pool	Customized	100%	ETH + DAI
ACO	American	Physical and Cash	Yes	Order Book	Standardized	100%	ETH + USDC
Primitive	American	Physical	Yes	Primitive Pool	Standardized	100%	ETH + DAI
Opium	European	Cash	Yes	Order Book	Standardized	fixed	ETH + DAI + ERC-20s
Pods	American	Physical	Yes	Uniswap Pool	Standardized	100%	ETH + DAI + aUSDC
Synthetix	not released	Cash	Yes	Synthetix Debt Pool	Customized	100%	SNX
FinNexus	European	Cash	Yes	Order Book & Pool later	Standardized & Customized later	Dynamic margin, less than 100%	FNX + WAN + BTC + ERC-20s later

Fig. 10 'Coinmonks' comparison of Option protocols. Source: https://medium.com/coinmonks/a-comparison-of-decentralized-options-platforms-140b1421c71c

3.7 Synthetics

A synthetic asset is one that has the same price as another asset. It is widely considered a derivative asset. In crypto, synthetic assets play a key role because they allow us to represent off-chain assets inside the blockchain. For example to buy gold with Eth, people should sell Eth for fiat currency and then go to the market to



sUSD
USD PRICE
$1.00
Tracks the price of a single US Dollar (USD). This Synth always remains constant at 1.
FEE: 0.30% ● LIVE

sEUR
USD PRICE
$1.13
Tracks the price of sEUR Euros through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sJPY
USD PRICE
$0.01
Tracks the price of sJPY Japanese Yen through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sAUD
USD PRICE
$0.72
Tracks the price of sAUD Australian Dollars through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sGBP
USD PRICE
$1.36
Tracks the price of sGBP Pound Sterling through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sCHF
USD PRICE
$1.09
Tracks the price of sCHF Swiss Franc through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sKRW
USD PRICE
$0.00
Tracks the price of sKRW South Korean Won through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sBTC
USD PRICE
$41,893.76
Tracks the price of sBTC Bitcoin through price feeds supplied by an oracle.
FEE: 0.30% ● LIVE

sETH
USD PRICE
$3,155.16
Tracks the price of sETH Ether through price feeds supplied by an oracle.
FEE: 0.25% ● LIVE

sLINK
USD PRICE
$27.55
Tracks the price of sLINK Chainlink through price feeds supplied by an oracle.
FEE: 0.85% ● LIVE

sADA
USD PRICE
$1.17
Tracks the price of sADA Cardano through price feeds supplied by an oracle.
FEE: 1.00% ● LIVE

sAAVE
USD PRICE
$208.63
Tracks the price of sAAVE Aave through price feeds supplied by an oracle.
FEE: 1.00% ● LIVE

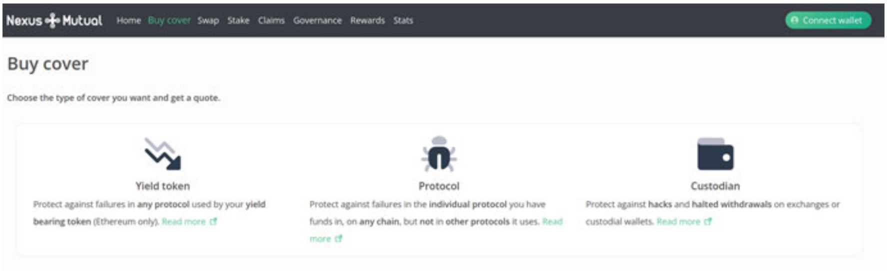
Fig. 11 Screen capture of the Synthetix interface

buy gold, thereby likely passing through centralized organizations such as banks and following KYC policies. If there is a synthetic token that represents gold, it is a simple on-chain transaction that becomes a fully decentralized transaction.

Synthetix is the main protocol on the Ethereum blockchain that allows the creation of synthetic assets called Synths. Synths examples are sXAU as a token that represents the gold price, sOIL representing the oil futures price, sNIKKEI tracking the price of Nikkei and sAAPL tracking the price of Apple stocks (see Fig. 11). There are also some inverse price tokens, such as iOIL, which represent the opposed behaviour of the price. To buy synthetic assets, first, the user must buy the Synthetix network token (SNX) and then stake it as a collateral with a 750% ratio (at the time of writing). Such a large ratio is important to keep the system healthy and avoid liquidations. Considering that all the synths are backed by the SNX token, when a user earns $1000 with a synth and another user loses $1000 with another Synth, then the system backing remains the same (Fig. 11).

3.8 Insurance

Insurance is a way to manage risks while hedging possible contingencies or losses. Typically, it is a contract called insurance policy between an insurer (mostly a company) and the insured (person or company) about the very well-defined circumstances in which compensation will be paid. Since the insurer and insured have opposite interests and the event covered could be debatable, both parties can use ordinary justice to solve a dispute.



Buy cover

Choose the type of cover you want and get a quote.

Yield token

Protect against failures in **any protocol** used by your **yield bearing token** (Ethereum only). Read more

Protocol

Protect against failures in the **individual protocol** you have funds in, on **any chain**, but **not** in **other protocols** it uses. Read more

Custodian

Protect against **hacks** and **halted withdrawals** on exchanges or custodial wallets. Read more

Fig. 12 Screen capture of the Nexus Mutual interface

Decentralization over the blockchain of traditional insurance is a very difficult endeavour. Actually, most projects are partially decentralized, such as Nexus Mutual, the leading insurance project, which is a UK company that requires a KYC policy to use the service. Apart from that, the rest of the operations are decentralized. How? Anybody can request the coverage of an event from the available types, as seen in Fig. 12. Anybody can stake NXM (the protocol token) to earn yield, thus providing liquidity for the payments of the coverage. Anybody (under specific features such as expertise) can act as a judge of the protocol claims, thereby earning tokens for the job. These are the three parties involved in the service, and each party has its own incentives (Fig. 12).

As in traditional insurance, the most sensible part of the business is the resolution of insurer claims. In summary, Nexus Mutual randomly chooses several judges who see the on-chain data to decide whether the claim is legitimate or not. If the judges agree to either support or deny the claim, they are rewarded; if one or very few of them disagree, then they are punished. Since cover conditions are very clear and on-chain data are fully open, there are few possibilities of honest mistakes.

At the time of the writing of this article, there were three types of covers in Nexus Mutual, namely, the yield token, which covers the staked tokens in yield farming protocols if they are lost due to errors in the smart contract on the protocol; the protocol, which covers losses in any protocol if it is hacked or it has smart contract errors; and the custodian, who covers technical errors (not human errors) made by token custodians in exchanges or wallets. The limitations of coverage came from the need for unambiguity and the need for on-chain data. The company that is behind the Nexus Mutual claims that they are planning to release more types. Oracles, smart contract improvements, and ecosystem maturity will support these changes.

3.9 Oracles

Blockchain information is public, anonymous and related to transactions, addresses or protocols. It is possible to know how many tokens an address holds, how many transactions a smart contract has processed or when a transaction has been made. Etherscan.io is a website that easily watches all the on-chain information obtained by the Ethereum blockchain. However, what if we need real-world information? In the smart contract section, we offered the example of a bet made on a Lakers game. To execute the smart contract, we need to know if the Lakers won or lost. However, we cannot simply grab the result of the game from somewhere online and write it on the blockchain. Why not? Because we could have interests in faking the reality or simply make a mistake when writing the result. We need a way to insert out blockchain information (off-chain) into a smart contract inside blockchain (on-chain) in a truthful way. We need an oracle.

Oracles bring off-chain information to on-chain without the need to trust a single party. They use the typical scheme in a blockchain of reward/punishment on a random group of nodes that check information outside the blockchain (mainly on the internet). If all of them offer the same information to the blockchain, it is considered truthful information; in this case, they are rewarded, and the information is written on the blockchain. If they do not offer the same information, then the nodes trying to fake information are punished. The requester of the information is who pays the effort (rewards to validators) to bring the information on-chain. This is how Chainlink works, which is the main decentralized oracle network.

Oracles are not a financial service like the rest of DeFi. However, they are the door to the real world and are responsible for enlarging what a smart contract over blockchain can do. On the other hand, they are considered a weak spot if they work badly, as some cases have proven (Qin et al., 2020). In summary, the power and future growth of DeFi will rely on the solidity of the oracles used.

4 DeFi and Startups

DeFi is an open-source, open-platform and permissionless technology that aims to remove middlemen. Is there space for businesses and startups in the decentralized paradigm? Absolutely yes, but in a very different way.

Most of the projects cited in this chapter were created by startups or by people who developed a startup later, some of them with venture capital investments. According to explodingtopics.com, the following are some of the most prominent DeFi startups:

- Uniswap, 2018 Brookling (USA), $11 million (Series A).
- Compund, 2017 San Francisco (USA), $25 million (Series A).
- MakerDAO, 2014 California (USA), $27 million (Series Unknown).
- Aave, 2017 London (UK), $24 million (Initial Coin Offering).
- Synthetix, 2017 Sydney (Australia), $12 million (Venture Round).

Additionally, DeFi protocols are growing exponentially in terms of total value locked (deposits peak $80 billion, see Fig. 13), fees generated (only Uniswap generates more than $1 million a day), or the market cap of the DeFi tokens (at the time of writing: $100 billion).

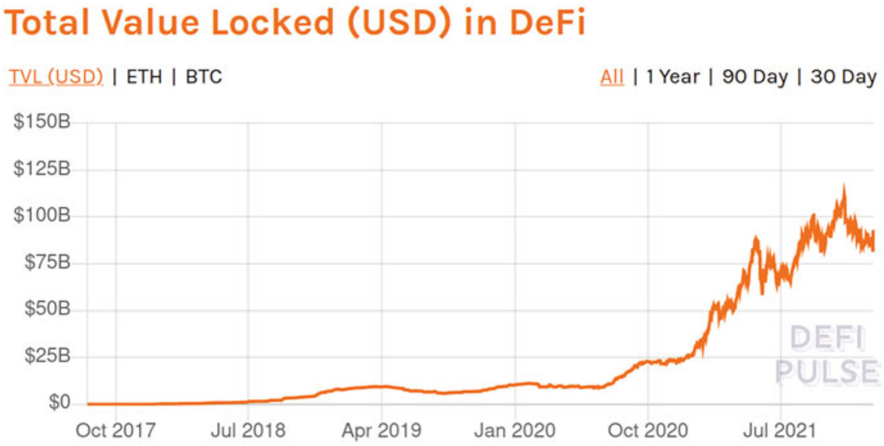


Fig. 13 Ethereum DeFi Total Value Locked in USD. Source: Defi Pulse

Creating a leading project in DeFi space is extremely difficult, not because of legal and capital entry barriers, as seen with traditional financial projects, but because of the need for very scarce and specialized talented people and new knowledge. Thus, the creation of a project from scratch will likely need capital to make a good team, at the bare minimum.

A typical way to create a software startup is to build and own the software and infrastructure (servers) and then sell the service to clients (SaaS model). In short, DeFi removes the owning part or at least transforms it. The code is public, and once released, the code is unstoppable (there are some nuances here that we cannot cover), and the infrastructure is the blockchain, which is not controlled by the company.

Regarding DeFi and startups, there is a dual reality, namely, the on-chain project and the off-chain company. The on-chain project is represented by a token or a smart contract that follows the rules of the blockchain and the contract. The off-chain company is a legal company that has some sort of influence in the community that created, impulsed, improved and expanded the on-chain project. The relation between the two is something that is unclear; in the roar of the DeFi explosion, this lack of clarity is not yet a public debate. However, it very likely will become one.

One of the most rewarding parts of building a DeFi project is token creation. Any project can create a new token or mint new tokens either before the launch of the project (ICO, IEO, IDO) (OECD, 2019) or after. Then, part of the allocation of the token goes to the team that built the project, the investors, the advisors or even the community. An example of Uniswap token allocation can be seen in Fig 14 and 15. For example Aave rises money selling tokens before a project launch, and Uniswap releases a token after several months of working without it. Again, avoiding many nuances, tokens can be seen as stocks of crypto projects. Traditional startups have a long journey to obtain a public IPO; however, in the DeFi context, companies could be public from day one (Figs. 14 and 15).

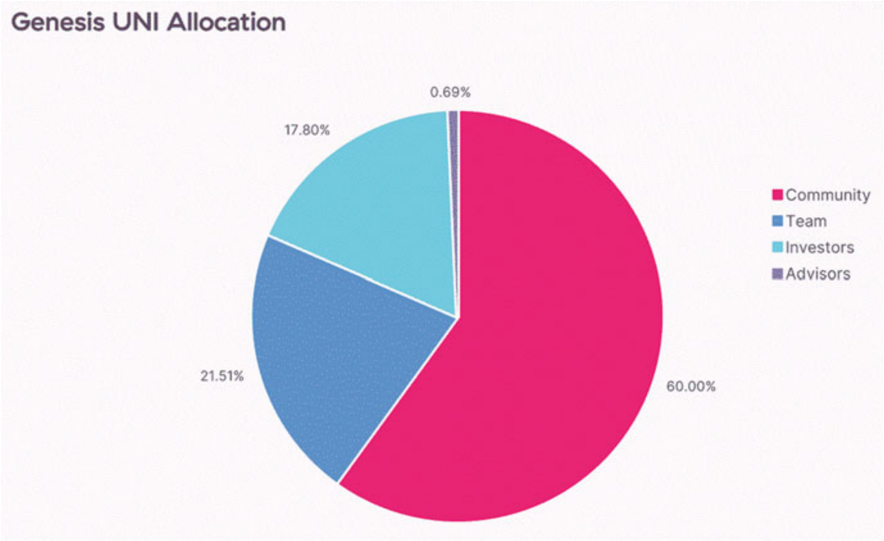


Fig. 14 UNI allocation. Source: Uniswap documentation

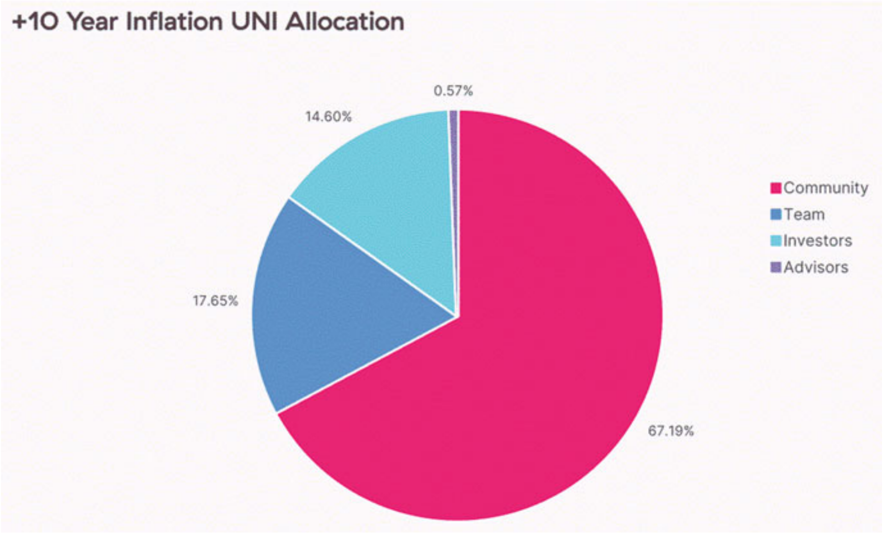


Fig. 15 UNI allocation. Source: Uniswap documentation

From a traditional business perspective, it seems very rare that the largest taxi company does not own a single car (Uber), that the largest accommodation provider does not own a single hotel (Airbnb) and that the largest media company does not generate content (Facebook). DeFi could be creating a paradigm in which financial software companies, instead of owning software and capital, manage communities of users that are ruled by public smart contracts on blockchains that align incentives to create markets of financial services, thereby reducing the need for trust.

References

Ante, L., Fiedler, I., & Strehle, E. (2021). The influence of stablecoin issuances on cryptocurrency markets. *Finance Research Letters, 41*, 101867.

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). *Comparative analysis of blockchain consensus algorithms*. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545–1550). IEEE.

Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money, 54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights, 13*, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151

Gudgeon, L., Werner, S. M., Perez, D., & Knottenbelt, W. J. (2020). *DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency*. Retrieved from https://arxiv.org/abs/2006.13922

José Luis Romero Ugarte. (2018). *Distributed ledger technology (DLT): Introduction*. Economic Bulletin, Banco de España, issue DEC, pp. 1–11. Retrieved from https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/2018/T4/descargar/Files/beaa1804-art26e.pdf

López-Cabarcos, M. Á., Pérez-Pico, A. M., Piñeiro-Chousa, J., & Šević, A. (2021). Bitcoin volatility, stock market and investor sentiment. Are they connected? *Finance Rsesearch Letters, 38*, 101399. https://doi.org/10.1016/j.frl.2019.101399

OECD. (2019). *Initial Coin Offerings (ICOs) for SME Financing*. https://www.oecd.org/finance/ICOs-for-SME-Financing.pdf

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2020). Attacking the DeFi ecosystem with flash loans for fun and profit. *arXiv preprint arXiv:2003.03810*.

Schär, F. (2020). Decentralized finance: On blockchain- and smart contract-based financial markets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3571335

Wang, Y. (2020). Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Yin, L., Nie, J., & Han, L. (2021). Understanding cryptocurrency volatility: The role of oil market shocks. *International Review of Economics and Finance, 72*, 233–253. https://doi.org/10.1016/j.iref.2020.11.013

Whitepapers

Aave, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf

Alpha Homora, https://alphafinancelab.gitbook.io/alpha-homora-v2/

Ampleforth, https://www.ampleforth.org/paper/

Bitcoin, https://bitcoin.org/bitcoin.pdf

Compound, https://compound.finance/documents/Compound.Whitepaper.pdf

DeFI Pulse Index, https://docs.indexcoop.com/our-products/defi-pulse-index

Dydx, https://docs.dydx.exchange

Enzyme Finance, https://docs.enzyme.finance/
Ethereum, https://github.com/ethereum/wiki/wiki/White-Paper
Hegic, https://github.com/hegic/whitepaper
Maker, https://makerdao.com/en/whitepaper/#overview-of-the-dai-stablecoin-system
Synthetix, https://docs.synthetix.io/litepaper
Uniswap, https://uniswap.org/whitepaper-v3.pdf
Yearn Finance, https://docs.yearn.finance/