IDX Insights Presents:

DeFi 101: A Guide to Decentralized Finance

A resource for fiduciaries and their clients to guide the understanding of DeFi as an asset class

Co-Authored by Ben McMillan and Josh Myers

1 TABLE OF CONTENTS

2 What is "DeFi"?

Decentralized Finance (or "DeFi") captures the ecosystem of applications (or "protocols") which are entirely built and distributed on cryptocurrency blockchains (mainly Ethereum…for now). These applications provide users with the same functionality as traditional finance (e.g., borrowing, lending, exchanging, etc) except that they're decentralized…meaning there is no trusted intermediary between parties. This function (of trusted intermediary) has been replaced by the consensus mechanism of the blockchain (which was the true genius behind the original Satoshi whitepaper). By cutting out the middleman, fees and transaction times are generally lower, and transparency is higher than performing the same function through traditional banking channels. There is also no central point of collapse (which was demonstrated in May of 2021 when a selloff in China resulted in every major centralized exchange temporarily shutting down while DeFi exchanges continued to operate). Therefore, this is just part of the reason DeFi has grown exponentially.

DeFi applications ("DApps") are built and deployed using smart contracts which are an innovative feature first introduced by the Ethereum blockchain. Like a co-op, these DeFi protocols are governed by the users that collectively own the tokens associated with a particular protocol. These Decentralized Autonomous Organizations ("DAOs") made up of token-holders, collectively decide how to govern the protocol.

3 Key Characteristics of DeFi

3.1 Non-Custodial

The defining characteristic of the DeFi ecosystem (and the single most significant departure from traditional finance) is the fact that there is no trusted intermediary or custodian. While non-custodial, distributed networks have several advantages (such as open, permissionless access and speed), it does introduce a layer of complexity for users. Because users serve as the custodian to their own wallets, it is up to them (or whoever they designate) to ensure the safety of those assets.

3.2 Open

The second significant characteristic of DeFi is that it is open and permissionless. The blockchain is global and borderless; and so too are the applications built on top of it. This means anyone can participate in the DeFi ecosystem without the frictions of centralized authorities and banking regulations. A wallet and an internet connection is all that stands between users and the features of the DeFi ecosystem.

3.3 Transparency

Transparency is crucial with decentralized networks because "code is law". There is no trusted intermediary to facilitate transactions or mediate disputes; this function is replaced by fully transparent smart contracts. This is crucial because it ensures that anyone using a protocol can determine the exact rules of engagement and under what specific conditions certain outcomes might be triggered (such as a margin call).

The inherent transparency of DeFi allows another key benefit: customization and improvement. Because the details of smart contracts are open for all to see, developers can enhance or build on top of existing applications. This has facilitated a speed of innovation within the DeFi ecosystem that can be orders of magnitude higher than within more traditional closed systems of finance. For this reason, many developers in the DeFi space refer to protocols as "money legos" because they are designed to be able to easily connect to each other.

3.4 Decentralized

DeFi protocols are built on public, decentralized networks like Ethereum. For this reason, these blockchains act more like an internet backbone (which, in this case, is run by thousands of computers, or 'nodes', globally); meaning there are no concerns around censorship or uptime. Assuming the network is sufficiently distributed, no central authority can control it or shut it down. This is the exact reason why many of the very early adopters of bitcoin were in highly controlled countries like China or Venezuela.

4 A Brief History of DeFi

When did DeFi begin and how (and when) did it grow so quickly? While there's no official start date for DeFi, it is worth highlighting a few key events that made it all possible.

The first, of course, was bitcoin: which launched in 2009 and, as we mentioned earlier, was groundbreaking in that it posited a way for trustless transactions to take place amongst two parties (i.e. no intermediary). This is achieved by replacing the trusted intermediary with a decentralized consensus mechanism. The technical aspects are beyond the scope of this resource but suffice it to say, this was a truly revolutionary idea…and one that catalyzed a new world of possibilities.

The first major enhancement to the generic blockchain project was the launch of the Ethereum blockchain: which was specifically designed with an added element that the bitcoin blockchain did not feature: smart contracts.

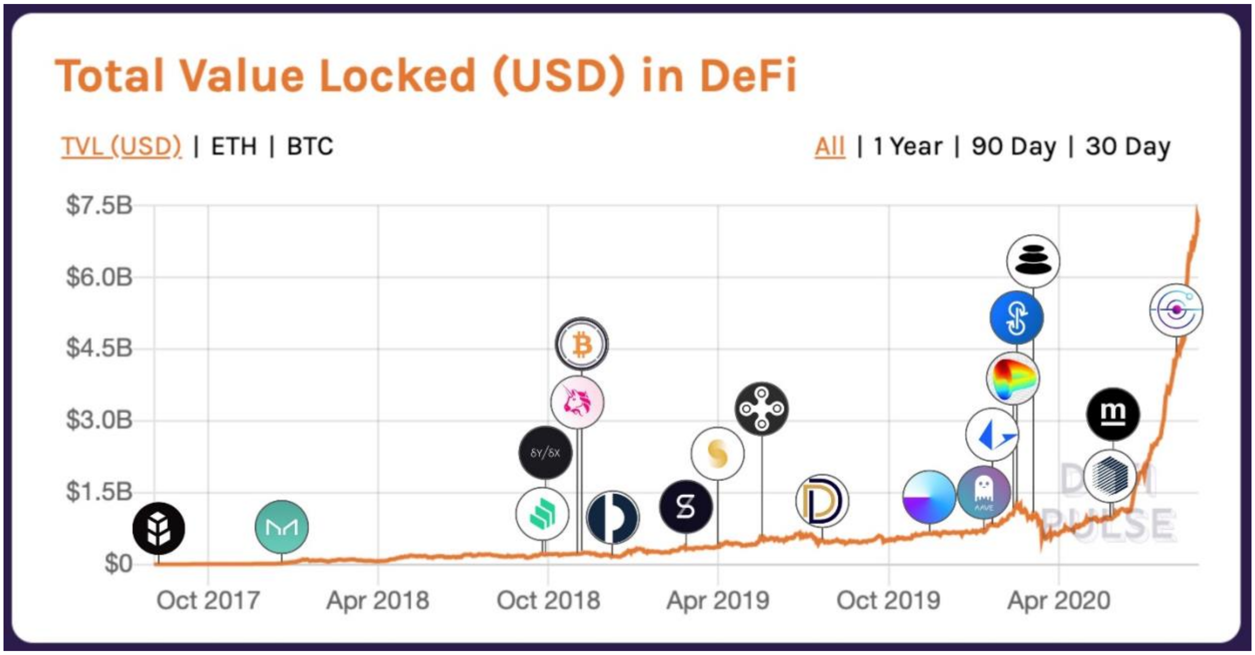
Bitcoin was singularly focused on facilitating a single outcome: sending digital money between two parties; but Ethereum was built with much bigger ambitions in mind. Vitalik Buterin created Ethereum in 2015 with a robust programming language (Solidity) and a standard for creating new tokens (ERC-20) that allowed developers to quickly start building full featured, robust applications.

4.1 The DeFi Ecosystem

Let's begin with one of the very first DeFi projects on Ethereum: Bancor. Bancor was established as the first blockchain-based "automated market maker" (AMM), which allowed users to exchange cryptocurrencies using a completely trustless, permissionless protocol of smart contracts deployed on the Ethereum blockchain.

A key innovation from Bancor was the idea of users interacting directly with smart contracts deployed on a decentralized blockchain as opposed to interacting directly with other users in a more traditional peer-2-peer model (e.g., Prosper or LendingClub). By creating pools of liquidity from users that were governed by smart contracts, ***other*** users could then interact with those liquidity pools to exchange digital assets (or eventually borrow and lend) without having to rely on a centralized trusted intermediary.

Bancor represented a revolutionary step forward in using smart contracts to actually power financial applications. The protocol takes its name from John Maynard Keynes' idea of a supra-national currency called "Bancor" to re-imagine international trade in the 1940's.[1]



Source: https://twitter.com/drwasho/status/1299195362456907776/photo/1

Almost a year later, Bancor was joined by Maker, a protocol designed to establish a decentralized cryptocurrency (called "DAI") that is pegged to the USD (otherwise known as a stablecoin). Like Bancor, Maker was entirely deployed as a set of smart contracts on the Ethereum blockchain. These smart contracts were maintained and governed by a Decentralized Autonomous Organization (DAO) which has come to be widely regarded as the early gold standard for how protocols could be

[1] https://en.wikipedia.org/wiki/Bancor_(cryptocurrency)

effectively governed in a truly decentralized and autonomous manner. *(listen to us talk to the Bancor folks here)*

Several months later, the DeFi ecosystem saw an explosion in protocols that allowed users to perform traditional finance functions like borrowing, lending, and exchanging digital assets; all entirely on the blockchain. This meant no account setup, no delay in sending assets and no approval from a trusted intermediary. The appeal was obvious and users quickly took note.

Right after the Maker Dao launched, there was approximately $100M of "total value locked" (TVL) between Bancor and Maker. As of writing, there is approximately $80BN of TVL across the various Defi protocols.

4.2 DeFi Summer

The explosion in DeFi protocols can be traced back to 2018-2019 but the explosion in the people using those protocols (the TVL) can be traced (largely) to the incentive program run by the Compound protocol in May 2020.

Compound was launched in 2018 as a decentralized platform for borrowing and lending digital assets. Borrowers would pay an interest rate to borrow tokens and lenders would receive those rates. In May 2020, the Compound platform started awarding additional incentives to both borrowers AND lenders on their platform in the form of Compound tokens (COMP). The COMP token gave the holder governance rights over the protocol and, as a result, had intrinsic value in the traditional sense. Importantly, the COMP token could be bought and sold on other exchanges. This meant that now, all users of the Compound platform were receiving an extra little subsidy that effectively made borrowing cheaper and lending more rewarding. This also kicked off a whole new era of "yield harvesting" where sophisticated users could simultaneously borrow and lend across certain digital assets (depending on the effective borrow/lend rates) and earn a very competitive yield…many times without having to incur market risk (i.e. with market neutral exposure). This incentive program proved so successful at attracting capital to the platform that virtually every other protocol adopted a similar program thus attracting a wave of new capital into the DeFi ecosystem.

One of the best examples of this was the decentralized exchange (“DEX”) called Uniswap which had launched back in 2018, but after seeing the success of Compound’s token launch, decided to retroactively reward the users of their platform with the UNI token (known as an “airdrop”). Uniswap’s monthly volume went from $169M in April 2020 to over $15B in September 2020. A massive increase of almost 100x.

As with any period of exuberance, there were several DeFi projects that weren’t successful (and some that were frauds), but by-and-large, 2020 was the year in which the idea of Decentralized Finance graduated from “interesting thought experiment” to “disruptive technology”.

5 DeFi Risks

Along with the explosion of DeFi, 2020 also saw a sea-change in institutional adoption of crypto assets. Particularly on the back of unprecedented levels of fiscal and monetary stimulus, investors started taking a much closer look at cryptocurrency assets as a store of value as well as a way to “own a piece of DeFi”.

That said, one of the defining hallmarks of decentralized finance (and digital assets, in general) is the idea of self-custody. Unlike traditional finance, investors within the crypto ecosystem (especially DeFi) have to act as their own custodian. As a result, hackers and unscrupulous actors no longer need to target Bank of America or JP Morgan to get access to users’ funds, they can target the users directly. This has led to a large number of phishing attacks that attempt to get in between a user and the security of their wallet.

Here are the best security practices to prevent being scammed from phishing:

Never share your recovery phrase

The first (and most important rule) to remember is that, when using a wallet, your recovery phrase (of 24 random words assigned when the wallet was created) is the ONLY way to access your digital assets. There is no reason this ever needs to be shared with anyone. When you connect your wallet to a DeFi protocol, it is NOT getting access to this phrase. As a result, hackers must convince the user to willingly give this out.

ALWAYS MAKE SURE THAT YOU INTERACT THROUGH OFFICIAL CHANNELS

Another common phishing attack involves setting up fake DeFi protocol sites (often with subtle spelling differences). While easy to prevent against, it does require another layer of vigilance. It's also worth noting that this is a popular phishing technique among traditional finance channels too.

STICK WITH ESTABLISHED DEFI PROTOCOLS

This is known as the "Lindy Effect" which posits that (with technology) the longer something has been around, the more likely it is to survive. This is important with any technology but particularly with DeFi protocols. Protocols that have been around for a couple years and have hundreds of millions (or billions) of dollars using them, are going to be more "battle tested" than those that just launched.

5.1 DEFI DUE DILIGENCE

Identifying risk is an important step towards safely navigating the DeFi ecosystem, and the next phase is understanding how to mitigate the unavoidable risks.

5.1.1 Smart contracts audit

Since "code is law" in the world of DeFi, it becomes paramount to understand the rules of the game, and equally as important to understand any vulnerabilities in the "code" that governs the game. In the same way that every traditional financial transaction is governed by a set of legal documents (and therefore interpretable by Lawyers), DeFi is governed by code. Instead of lawyers, that function now falls on programmers who can interpret and deploy that code (which in the case of ERC-20 contracts is *Solidity*). That's not to say that having a staff of Solidity programmers is a requisite for participating in DeFi (it's almost entirely an open-source community with robust self-policing mechanisms ***if*** users are willing to seek them out), but knowing how the machine operates can certainly lend safeguards and advantages. Additionally, a cottage industry of "code audit" firms have sprung up to offer 3rd party assessments of protocol code, which provides a "necessary but not sufficient condition" for participation. At the end of the day, the best way to ensure that you are participating via a robust set of governing smart contracts, remains sticking with protocols that have been around the longest and have survived the test of time; the "Lindy Effect".

5.1.2 DeFi monitoring tools

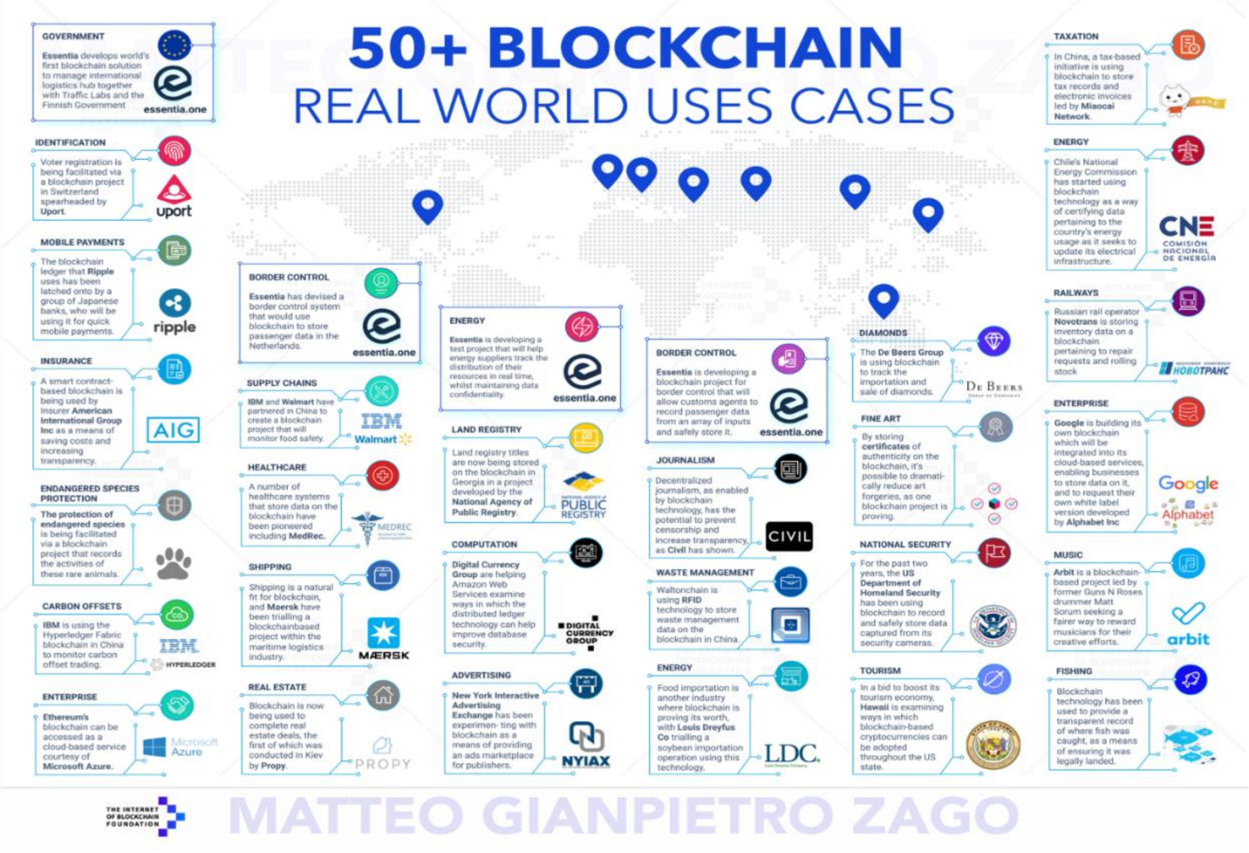
If understanding your participation is the first phase, then accurately monitoring your participation naturally follows in sequence. Since there is no custodian or trusted intermediary providing reporting, that function ultimately resides with the participant. Furthermore, because the code-driven protocols trigger events (such as liquidations) immediately upon defined conditions being met, there are no courtesy calls from a prime brokerage desk giving you time to cure your margin requirement…code is law. As a result, many sophisticated users have written their own smart contracts to monitor and react to certain events automatically so that if, for example, a collateralization limit gets close to a breach, the investor (or more likely the code they deployed) can adjust accordingly before the code of the protocol takes effect.

It’s important to note that the investor (participant) is not entirely on their own when it comes to applying these smart contract oversights. In fact, the 2020 surge in development by many top borrowing and lending protocols, such as Aave, have provided for alerts and reminders built in for their users when they are approaching a liquidation threshold. They coined the term “Health Factor” for the industry, which is similar to a mortgage borrowers Loan to Value (LTV) ratio.

6 The Future of Finance

As mentioned, DeFi has proven it’s utility. Like the internet in its early days, it took some time before it was clear how ubiquitous the technology would ultimately be. Decentralized Financial applications are showing a very similar trajectory. Like the internet, the open-source nature of DeFi means that the rate of innovation is exponential. Particularly as the technology of the underlying blockchains’ continues to develop and improve, such as the recent London Fork upgrade to Ethereum…as well as the, much anticipated, “Ethereum 2.0” upgrade (in 2022).

Increasingly more use cases are beginning to emerge, such as insurance, supply chain logistics, real estate, rare collectibles authentication, etc.



50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

INSURANCE
A smart contract-based blockchain is being used by insurer **American International Group Inc** as a means of saving costs and increasing transparency.

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure**.

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramati-cally reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION
MATTEO GIANPIETRO ZAGO

As investors saw with the newly emerging "internet stocks" of the 90's, the disruptive technology phase is often accompanied with huge amounts of speculative hype. Considering the plethora of Pets.com anecdotes, and the fact that a large number investments ("Companies") in the "Dot Com Mania" resulted in significant capital loss, the survivability and the value of disruptive technologies can be difficult to see through all of the speculation; still, many would argue that the value created by the Amazon's, the eBay's and the Google's more than compensated for the risks that were assumed in their early stages of development. We too expect that in the years ahead, most investors will look back at DeFi's growth curve in the same way that many look back on "the internet", and conclude that the rapid evolution and societal adoption were a foregone conclusion.