crypto.com

Decentralized Finance

A Brief Introduction to DeFi

April 2020

Research and Insights

DeFi Report

Senior Research Analyst

Kendrick Lau

RESEARCH DISCLAIMER

This report alone must not be taken as the basis for an investment decision. The user assumes the entire risk of any use made of this information. The information is provided merely complementary and does not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind. The views expressed therein are based solely on information available publicly/internal data/other reliable sources believed to be true. This report includes projections, forecasts and other predictive statements which represent Crypto.com's assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. Opinions expressed therein are our current opinion as of the date appearing on the report only.

No representations or warranties have been made to the recipient as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions contained in this report or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

The reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. Persons into whose possession the reports may come are required to observe these restrictions.

Contents

1. Executive Summary

Welcome to the beginning of our research series on DeFi! We hope you will come to understand the world of decentralized finance more after reading this report.

Key Takeaways

- Decentralized finance, or DeFi, refers to financial services, including lending, exchanges, investment, stablecoins, and more, that are built on public blockchains and smart contracts, most commonly Ethereum;
- The main benefits of DeFi is that financial services become trustless, censorship resistant, permissionless, and open source. DeFi can in theory make platforms more secure, more resistant to manipulation, accessible for anyone, and transparent;
- Although most DeFi protocols have achieved a high degree of architectural decentralization, full political decentralization is hard to achieve. As such, most protocols are still partially centrally governed by central developer teams or foundations;
- The most popular use of DeFi is for borrowing and lending, allowing users to put their crypto assets to work to earn interest;
- DeFi's main drawback is smart contract risk, where an attacker could exploit vulnerabilities in smart contracts to steal user funds. However, we believe any attack presents an opportunity for DeFi to mature and improve security practices;
- Other drawbacks of DeFi are that it is limited by blockchain throughput and that there could be regulatory oversight on the horizon since it currently operates in a regulatory gray area. Improvements in these areas could help DeFi grow further

If you would like to learn more about DeFi, feel free to head over to our Research Hub, where we have already published and will be publishing more content on DeFi.

2. Introduction

2.1 What is DeFi

Decentralized finance, or DeFi, refers to financial services that are built on public blockchains and smart contracts, with the use and control of the system distributed amongst many different parties. The area has quickly emerged as one of the primary use cases for Ethereum. Similarly to how bitcoin established the first decentralized currency, DeFi players are attempting to build a decentralized, trustless financial system, offering services such as lending, exchanges, investment, stablecoins, and more, not just for cryptocurrencies, but possibly for all financial assets, too.

DeFi began to gain widespread popularity beginning last year, and since then, has grown rapidly, with over US$700 million worth of ETH locked in DeFi applications as of today.

2.2 Why DeFi

Why does DeFi need to exist and why does it have the potential to change the face of the crypto industry and the financial landscape? To put it simply, DeFi makes all financial interactions trustless and permissionless. This removes the main downsides of interacting with centralized services: namely, a lack of transparency, accountability, and custody risk.

In the crypto industry, centralized exchanges have been the predominant way for people to gain access to products and services. Users who wish to gain access to trading services must first go through an account opening process, giving their personal information. Furthermore, they also have to give up custody of their assets and risk it being lost in the event of a security breach, with little recourse if this happens.

With the numerous high profile hacks and trust issues experienced over the years, DeFi aims to give users an alternative by removing the need to trust a third party at all. This is achieved this by building services using smart contracts in an open, permissionless, and decentralized manner.

3. What is DeFi

Now that we have gone through a brief introduction on what DeFi is and why it exists, we will now explain the core principles of DeFi that make it attractive, and what types of services are available.

3.1 Types of Decentralization

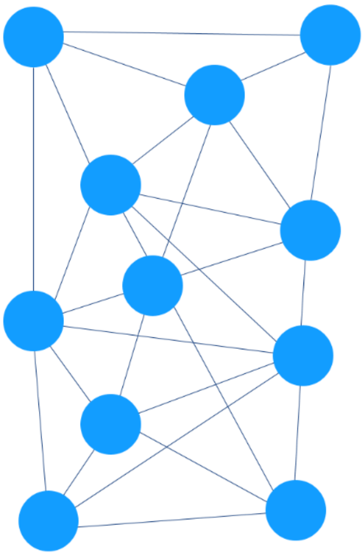
Before going into reasons why decentralization is important, we must first describe the two main types of decentralization: 1) architectural decentralization, and 2) political decentralization.

Architectural Decentralization

Architectural decentralization refers to the number of physical nodes that partake in the operation of the system. As a simplified example, the bitcoin network is decentralized because many different nodes work independently to validation the transactions. Nodes also monitor each other to ensure that no collusion is happening. This is important since DeFi runs on public, decentralized blockchains such as Ethereum. We would argue that architectural decentralization is the defining hallmark of DeFi protocols.

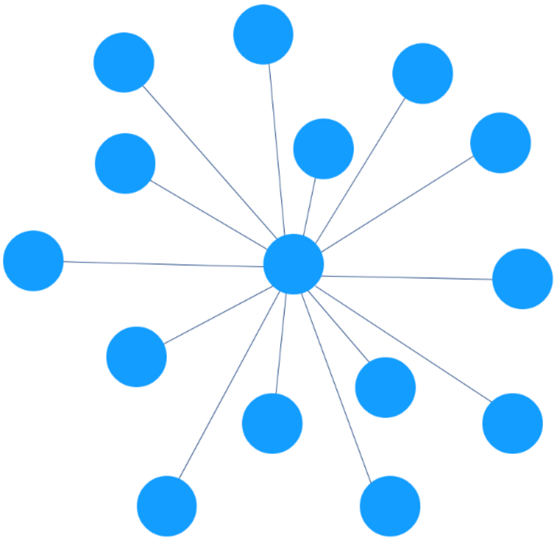
Architecturally Decentralized

All nodes can communicate with each other. System does not rely on any single node



Architecturally Centralized

All nodes communciate with just a central node. Without central node, system breaks down



Political Decentralization

Political decentralization refers to how many individual entities control the rules of the system. To give a simple example, in a direct democracy, every person has one vote to directly influence policy changes in that country, so it is highly politically decentralized. This is in contrast to a dictatorship where policy is decided unilaterally by one person or party.

Although political decentralization is a desirable trait, in practice it is hard to fully achieve since it requires developers to first implement the system, and then hand over its governance and maintenance to a distributed group of stakeholders who may not fully understand how the system works, or lack the technical expertise to build and maintain code. For this reason, DeFi protocols today that have achieved full political decentralization are few to none.

To read more about the concepts of decentralization, feel free to read this article by Vitalik Buterin.

Degrees of Decentralization

There are many other aspects of decentralization that intersect with the overarching types above. These relate to:

- Custodial arrangements;
- Price oracle feeds;
- Liquidity provision;
- Governance;
- Development

It is important to note that centralization is not black and white. Instead, it exists as a spectrum, from fully centralized to fully decentralized, with most protocols and products existing somewhere in between.

3.2 The Importance of Decentralization

Why is it so important that DeFi creates financial services where its usage and control are decentralized? We will go through each benefit as it pertains to DeFi.

Trustless

Because financial services inherently deal with users' money, trust and security are very important to the sustained function of these systems. Once trust is lost, whether warranted or not, it is very hard to regain and can lead to the debilitating collapse of entire financial systems.

History is littered with examples of this happening – take the failures of monetary regimes in Venezuela, Argentina, and Zimbabwe leading to hyperinflation and economic recession, or economic mismanagement leading to bank runs in Greece. Trust in centralized cryptocurrency systems is similarly important – users have to trust that centralized exchanges will keep their funds safe, while users of Tether (USDT) must trust that there is actually US dollars backing each USDT. Given the lackluster track record that centralized systems have had, it is natural to wonder whether there is a better system.

Hence DeFi was created. Assets are escrowed in smart contracts on the blockchain and cannot be extracted unless certain conditions are met. Furthermore, protocols are designed such that stakeholders are incentivized to act in a way that benefits the system, removing trust from the equation altogether.

Censorship Resistance

Censorship resistance refers to how difficult it is to tamper with a system's operation for any reason, be it financial or political. Since the operation and control of ideal DeFi systems is decentralized, they can be much more censorship resistant than their centralized counterparts.

Centralized systems can easily be interfered with, manipulated, or shut down by external parties. For example, governments could shut down the centralized servers of exchanges, blocking them from serving users or from functioning altogether. Similarly, the exchange's owners can manipulate internal mechanisms to benefit themselves and leave users none the wiser.

An ideal DeFi system reduces the possibility of these forms of censorship, by distributing both the architecture and governance of its protocol. Because DeFi protocols are run on public blockchains like Ethereum, the only way to halt their operation is by shutting down the Ethereum network. This task is much more difficult than shutting down a single exchange. Similarly, distributed governance powers make it very hard for any single party to gain control over DeFi protocols and tamper with its operation.

Due to this trait, DeFi systems inherently have the potential to be more secure and tamper-proof than their centralized counterparts.

Permissionless and Borderless

DeFi protocols are, almost without exception, permissionless – anybody can participate in their governance or use. Since no personal information is required, country and regulatory restrictions cannot be easily enforced by extension.

This makes DeFi services much more accessible than centralized financial services, which require potential users to jump through all kinds of hoops before access is granted.

Of course, this raises the natural question of DeFi's use by criminals and money launderers, and what regulators will do to combat this. We will address the topic of regulatory risk in the Analysis section.

Open Source and Transparent

One of the core philosophies of DeFi is that everything should be open source. There are a few reasons for this:

Firstly, open source code can be audited to test for security vulnerabilities that may put user funds at risk. Secondly, it allows anyone to interpret how the system works, letting the user base know what to expect on a consistent basis without arbitrary and hidden changes. Lastly, it allows the community to recreate ("fork") a protocol in case the original becomes compromised, or simply if someone comes up with a better version of it.

This openness gives DeFi a level of robustness and iterative improvement capacity that cannot be found in centralized alternatives.

3.3 DeFi Subcategories

Almost any financial service you could think of has its DeFi counterpart. We will go through the most prominent categories below. Note that not all the examples we give below are fully decentralized, so make sure to do your research or read our DeFi Reports on them before trying them out!

Stablecoin

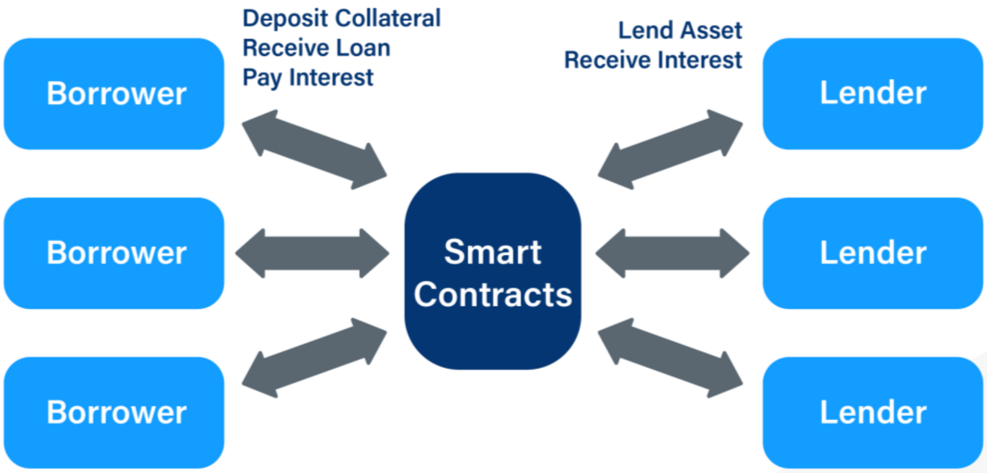
A common medium of exchange and unit of account is critical to any well-functioning financial ecosystem. DeFi is no different, but the most widely used cryptocurrencies are often volatile in nature, making them ill-suited as transactional tools. Hence, stablecoins were invented as cryptocurrencies that maintain a constant value.

The most well-known stablecoin is fiat-backed Tether (USDT), which promises to maintain 1:1 ratio of USDT to USD since every USDT is theoretically backed by $1 USD. This obviously requires the user to trust Tether with the custody of US dollars. But in the past, there have been doubts on whether Tether is actually fully backed by dollars, leading to unwanted fluctuations in the value of USDT.

the Dai stablecoin (DAI) was created by MakerDAO to eliminate the necessity for third party custody. Each DAI is collateralized by at least 150% of its value in crypto, and is the only widespread, trustless, non-custodial stablecoin on the market today. This has made it a mainstay of the DeFi landscape, used commonly in other DeFi protocols as a basic building block.

Borrowing and Lending

Perhaps one of the most fundamental of all financial services, borrowing and lending platforms are the most common use case for DeFi today. These protocols aim to replace financial intermediaries such as centralized exchanges and banks by building peer-to-peer lending platforms through the use of smart contracts.



Similar to a bank, these platforms take assets from users and allow them to earn interest by lending them out to borrowers. The difference here is that there is no credit officer reviewing your loan application – smart contracts set the terms of the loan, allowing the loan to occur automatically and instantaneously once the conditions are met (typically once sufficient collateral is deposited).

Because the system is built on blockchain, anyone with an Ethereum address can access credit without going through an arduous account opening or credit review process. Borrowed funds can also be transferred anywhere since the funds are credited directly to the user's wallet, unlike in centralized exchanges where margin loans must remain on the exchange's systems.

DeFi lending platform examples:

MAKER Compound AAVE

Feel free to read our reports on Maker and Compound here.

Exchanges

Unlike centralized exchanges, decentralized exchanges (DEX) perform transactions in a peer-to-peer manner through the use of smart contracts. This allows users to trade without relying on a third party, eliminating a layer of fees that go to paying the costs of the exchange. Furthermore, there are no account opening processes or withdrawal fees. Unlike centralized exchanges, these DEX will not face service interruptions as long as the Ethereum network is operational.

Note that there are two exchange models used by decentralized exchanges: *Order book* and *token swapper* models.

Order book DEX are similar to centralized exchanges, where users' orders are matched against an existing order book.

Token swappers pool liquidity from users in a decentralized manner. They allow users to trade directly against the system, eliminating the need for an order book.

Order book DEX examples:

IDEX δY/δX

Token swapper examples:

UNISWAP Bancor

kyber network

You can read more about Uniswap here.

Asset Management

Traditionally, if you wanted to have someone manage and invest on your behalf, you would need to give up custody of your assets. With all the scams and Ponzi schemes that have resulted in lost investor funds, it is not surprising that a DeFi solution for asset management also exists. These protocols allow users to allocate assets to different trading strategies in a non-custodial and trustless way.

DeFi asset management examples:

Set

MELONPORT

Derivatives

Derivatives are designed to replicate holding the actual asset without physically doing so, or to simulate different ways of investing in an underlying asset (i.e. derivatives giving short or leveraged exposure).

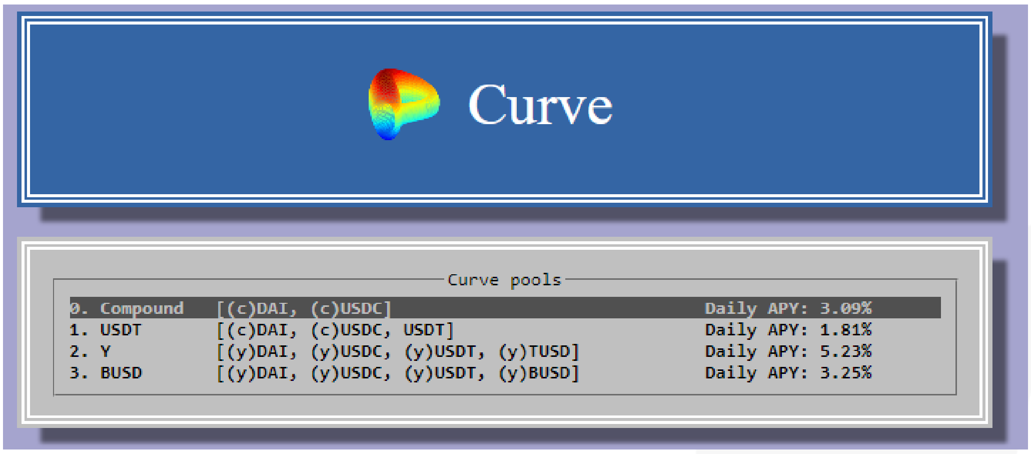
In traditional finance, there are derivatives for stocks and bonds. Similarly in the crypto industry, centralized exchanges offer bitcoin futures, options, and so on. In the DeFi space, Synthetix is a platform that allows users to trustlessly issue and trade synthetic assets that mimic the performance of both crypto and real world assets like fiat and gold.

SYNTHETIX

Non-Custodial Wallet

No matter how good a product’s technology is, if a user-friendly interface doesn’t exist, it will be difficult for the product to reach mass adoption.

DeFi protocols are still used only by a niche subset of the community due to their relative complexity, with complex interfaces to match. For example, check out the main interface of curve.fi below, which is difficult to navigate for all but the most hardened DeFi veterans:



```
Curve pools
0. Compound    [(c)DAI, (c)USDC]                          Daily APY: 3.09%
1. USDT        [(c)DAI, (c)USDC, USDT]                    Daily APY: 1.81%
2. Y           [(y)DAI, (y)USDC, (y)USDT, (y)TUSD]        Daily APY: 5.23%
3. BUSD        [(y)DAI, (y)USDC, (y)USDT, (y)BUSD]        Daily APY: 3.25%
```

The missing linkage is therefore a user-friendly non-custodial wallet (NCW). NCW can provide the following benefits to users:

- Non-custodial crypto asset storage;
- Smooth user experience;
- Facilitate interoperability between DeFi protocols

NCW examples:

METAMASK

argent

Others

There are many other markets for which DeFi solutions are being developed, such as prediction markets, insurance, and DeFi infrastructure. For example, Nexus Mutual is a decentralized insurance platform that lets users buy and sell insurance on DeFi risks. In the prediction markets, Augur is growing in popularity as a platform for betting. There are also protocols to facilitate DeFi as a whole; for example, 0x is a relayer protocol that supports decentralized exchanges.

We will not describe these in detail in this article, but do stay tuned for further content on our Research Hub.

0x AUGUR

Nexus Mutual

Beyond Ethereum

All the DeFi protocols we have introduced above are Etheruem-based. But DeFi need not be built on Ethereum. As long as they are decentralized and finance-related, we can still categorize them as DeFi.

Examples of non-ETH DeFi:

Lightning Network® Newdex

Ren

4. Analysis

Now that we have an understanding of what DeFi is and its main benefits, let's explore some of its drawbacks and downsides.

4.1 Downsides of DeFi

As we have just described, DeFi has the potential to overhaul the existing financial services as we know them, carrying with it the many benefits that made cryptocurrencies attractive in the first place. But what are the drawbacks of DeFi, and isn't it more widely utilized? We will go through what we view as DeFi's main disadvantages one by one.

Smart Contract Risk

Perhaps the most significant drawback with DeFi is that it introduces smart contract risk. Instead of centralized custody and servers, users of DeFi have to trust that the smart contracts underlying the protocol do not have any vulnerabilities that could put users' assets at risk.

The most prominent types of exploits and attacks that have occurred recently involve the manipulation of external price feeds for assets within protocols, called price oracles.

This occurred twice in February 2020 on the DeFi lending platform bZx, where an attacker or attackers manipulated the oracle price of collateral on two occasions. This allowed the attacker to borrow much more than they were supposed to be able to, leaving bZx lenders with combined losses of almost US$1 million.

A similar vulnerability was exposed with Synthetix in 2019, where a trader on the Synthetix platform was able to manipulate the price feed of KRW, resulting in a profit of US$1 billion in less than an hour. Fortunately, the trader agreed to forgo his profits in exchange for a bug bounty since he was unable to cash out his profits.

Most infamous, though, is the 2016 attack on one of the original DeFi protocols, the DAO (Decentralized Autonomous Organization). An attacker drained over 3.6 million ETH (worth $72 million at the time) from the DAO's smart contracts. The Ethereum community agreed return funds to DAO investors via a "hard fork" of the network into what is now known as Ethereum (ETH) and Ethereum Classic (ETC).

Detractors point towards these hacks as reasons for why DeFi is no better than centralized exchanges. Each attack gives rise to a slew of articles and arguments on why DeFi is fatally flawed, and will always need centralized interference to reverse damage from attacks.

In our view, however, these attacks are a necessary part of an industry that has yet to reach maturity. Each attack on DeFi exposes development flaws, reducing the odds that future projects will make similar mistakes. Attacks also encourage more rigorous security audits and bug bounty programs to catch vulnerabilities before they result in user losses. Over time, DeFi will likely become increasingly secure, ultimately achieving a level of security and user trust that centralized platforms will be hard pressed to match.

Limited by Blockchain Speed

If you have ever tried using DeFi applications, you might have noticed a significant delay between transaction requests and confirmation. This is because every transaction and interaction is subject to Ethereum network confirmation, which can take anywhere from a few seconds to ten minutes depending on network congestion. This type of delay can be a deal breaker for users who prioritize speed and certainty.

But with the release of ETH 2.0 expected in July 2020 promising higher throughput and confirmation speed (read more in our University article), it is hopeful that dApps will greatly improve their speed.

Regulatory Risk

DeFi operates within areas that traditionally have significant oversight from governments and regulatory bodies around the world who wish to protect unknowing users from scams and risky products.

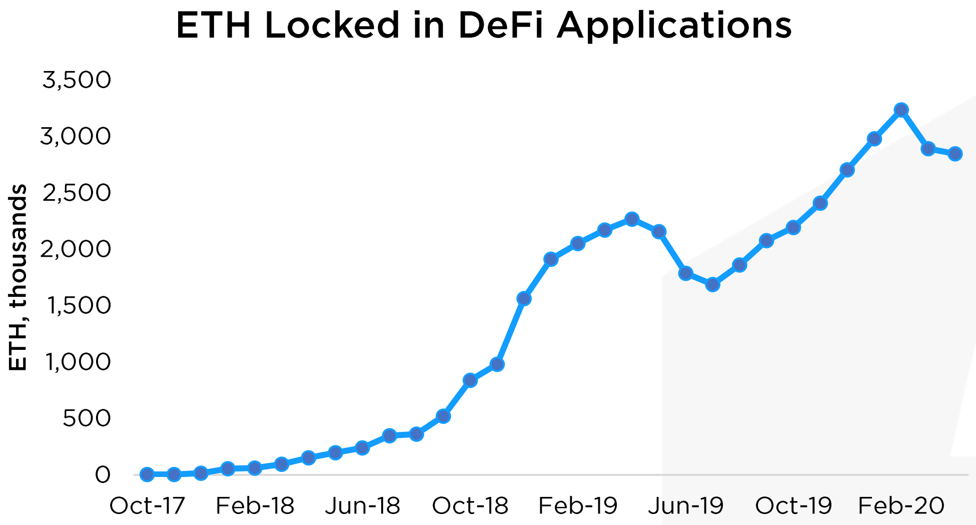
However, since DeFi protocols for the most part have been designed to be permissionless from day one, so anyone in any country can theoretically access them with no regulatory or compliance barriers.

This sounds great from a user’s perspective but to regulators, DeFi sounds awfully like a haven for criminals and shady individuals to gain access to financial services. Since there has been no meaningful regulation developed around DeFi services, it is safe to say that DeFi operates within a regulatory and legal gray area.

Judging by the current regulatory trends of greater know-your-customer (KYC) and other compliance requirements, we suspect that DeFi will fall under the scope of global regulators as it grows in scale. As such, DeFi could eventually become at least partially permissioned, using decentralized identity and address checking services to block certain users from its use.

This is obviously not a great outcome for users who wish to remain anonymous, but on the other hand, it could mean greater adoption of DeFi from large financial institutions and the general public.

4.2 Statistics



Since 2017, the DeFi space has grown rapidly, with the ETH locked in DeFi applications growing from 5,000 in late 2017 to 2.8 million as of April 2020.

We can see two instances of large scale asset outflows from DeFi. The first occurred in mid-2019 in the aftermath of the Synthetix oracle exploit. The second occurred recently in February 2020 after the bZx attacks.

5. Conclusion

In summary, DeFi offers a new way of conducting financial transactions and could herald in the new era of growth for the crypto industry. Eventually down the line, we could even see DeFi principles apply to traditional financial markets, as we see more central banks creating programmable digital currencies (read our article on CBDC here). We are excited to see where DeFi takes us as it grows and matures.

Key Takeaways

- Decentralized finance, or DeFi, refers to financial services, including lending, exchanges, investment, stablecoins, and more, that are built on public blockchains and smart contracts, most commonly Ethereum;
- The main benefits of DeFi is that financial services become trustless, censorship resistant, permissionless, and open source. DeFi can in theory make platforms more secure, more resistant to manipulation, accessible for anyone, and transparent;
- Although most DeFi protocols have achieved a high degree of architectural decentralization, full political decentralization is hard to achieve. As such, most protocols are still partially centrally governed by central developer teams or foundations;
- The most popular use of DeFi is for borrowing and lending, allowing users to put their crypto assets to work to earn interest;
- DeFi's main drawback is smart contract risk, where an attacker could exploit vulnerabilities in smart contracts to steal user funds. However, we believe any attack presents an opportunity for DeFi to mature and improve security practices;
- Other drawbacks of DeFi are that it is limited by blockchain throughput and that there could be regulatory oversight on the horizon since it currently operates in a regulatory gray area. Improvements in these areas could help DeFi grow further

If you would like to learn more about DeFi, feel free to head over to our Research Hub, where we have already published and will be publishing more content on DeFi.

6. References

Biggs, J. (2019). *Synthetix Trader Rolls Back Broken Trades That Netted $1 Billion Profit.* Coindesk. Retrieved from https://www.coindesk.com/synthetix-trader-rolls-back-broken-trades-that-netted-1-billion-profit

Buterin, V. (2017). *The Meaning of Decentralization.* Medium. Retrieved from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

DeFi Pulse. (2020). Retrieved from http://defipulse.com

Facts, C. (2020). *"Ethereum 2.0" Explained.* Retrieved from https://cryptocurrencyfacts.com/ethereum-2-0-explained/

Falkon, S. (2017). *The Story of the DAO — Its History and Consequences.* Retrieved from https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Foxley, W. (n.d.). *Everything You Ever Wanted to Know About the DeFi 'Flash Loan' Attack.* Coindesk. Retrieved from https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack

Mitra, R. (2019). *DeFi - What in the world is Decentralized Finance? The Most Comprehensive Guide.* Blockgeeks. Retrieved from https://blockgeeks.com/guides/demystifying-defi-ultimate-guide/

Trustology, C. (2019). *Enabling cost-effective, compliant access to decentralized finance (DeFi).* Retrieved from https://trustology.io/wp-content/uploads/2019/11/Chainlink_Trustology_FINAL.pdf

crypto.com

e. contact@crypto.com