1 Introduction

If we can email virtually anybody in the world, why can't we send them money just as easily? Or offer them a loan? These questions are the foundation of Decentralized Finance's (DeFi) beliefs, activities and objectives. In short, DeFi refers to an ecosystem of financial applications that are built on top of a blockchain. Its common goal is to develop and operate in a decentralized way – without intermediaries such as banks, payment service providers or investment funds – all types of financial services on top of a transparent and trustless blockchain network.

The DeFi field is currently experiencing an incredible surge. More than two billion US Dollars (USD) – a value that doubled over the last weeks in June 2020 – have already been deployed (»locked-in«) across a variety of DeFi applications that offer lending and borrowing services, exchange services, monetary banking services (e.g. the issuance of stablecoins), tokenization services, or other financial instruments such as derivatives and prediction markets. In that sense, DeFi is not a specific thing, but more a loosely defined collection of ideas and projects to reshape financial services through blockchain technology, thereby removing the middlemen.

Its disruptive potential has brought DeFi into the spotlight of the blockchain and fintech communities, and increasingly also to the attention of traditional financiers and policymakers. However, it appears that these different parties often lack a common understanding of what DeFi is and is not, and further, of how DeFi can overcome major technical, operational and regulatory obstacles that challenge its further development. We firmly believe that DeFi's growth and success is inextricably linked to greater dialogue, cooperation, and integration with political stakeholders, regulatory supervisors, traditional finance, and fintech.

As a cross-industry business association and Europe's biggest tech network, we not only want to contribute to this trajectory, but also to create and support cooperation in the first place. This is why we decided to write a whitepaper as groundwork for further discussions, network meetings, and policy consultations. After these introductory words in chapter 1, the paper continues with a short recap of blockchain technology in ↗chapter 2. This serves as the basis for ↗chapter 3, which explains how DeFi builds financial services bottom-up. ↗Chapter 4 deep dives into three of the most prominent DeFi real world applications, namely Maker, Compound and Uniswap. ↗Chapter 5 takes a closer look into the major risks and obstacles that the DeFi ecosystem has to overcome, for example, technical limitations (bugs, hacks, throughput, UX etc.) and also regulatory and operational bottlenecks. ↗Chapter 6 closes the whitepaper with a mid-term outlook of DeFi's path forward in the coming years.

The goal of this paper is to reach as many people from different backgrounds as possible, explain the basics of DeFi, and raise interest in this promising young technology field. For newcomers, this might be the first step. But we hope that you, like us, will build on these insights and take further steps to become a DeFi enthusiast. So let's get started!

2 Blockchain technology – foundation for DeFi

How is it possible that investors entrust more than two billion USD to decentralized applications, against which they have no legal recourse and which are often less than three years old? Where does this trust come from? The answer lies in the technology: blockchain technology. In the case of DeFi, it is usually the Ethereum blockchain that provides this level of trust. While we assume that readers of this paper are familiar with Bitcoin and blockchain in general, we will very briefly recall some important aspects below.

Bitcoin

Bitcoin is the world's first blockchain. Its sharp price increase end of 2017 made Bitcoin finally famous to broader groups of society. The two core properties of Bitcoin are scarcity and security.

- It is scarce because there will never be more than 21 million Bitcoin issued. When Bitcoin was invented in 2009, it was the first and only limited digital resource that could not be copied as often as desired, as opposed to a digital picture or text. From an investment perspective, Bitcoin today is referred to as »digital gold«, as it is primarily considered an alternative and uncorrelated investment asset. It has never been hacked and trades today (as of July 2020) at a price of more than 9,000 USD, resulting in a market cap of 127 billion USD.

- The security part is a bit more complex: Bitcoin is based on the blockchain technology. But what is a blockchain? The entire history of Bitcoin transactions is stored in a transaction list, the ledger. Each new transaction is added and attached to this ledger. However, this is not done on a single transaction basis, but in blocks. This chain of blocks is where the name Blockchain stems from. If this blockchain were stored in a data center that was then successfully attacked, the attack could put the security of the whole network at risk. It would only take one successful attack to discredit the blockchain and all of its listed blocks and transactions. Therefore, the ledger is stored in a decentralized way on multiple computers. It is currently estimated that there are about 10,000 active full nodes (i.e. computers storing a full copy of the blockchain), that are distributed all over the globe. Attacking Bitcoin would require attacking all computers storing the blockchain (or a large number of these computers) at the same time. This, in addition to cryptography, is the major reason for Bitcoin's security.

Bitcoin serves a fundamental and fairly easy use case by storing value through time and transacting value if necessary. The user can do no more than receive, store, or send units of Bitcoins. One major weakness (or, depending on the perspective, a major strength) of Bitcoin is its significantly limited programming language that is incapable of implementing complex computational logic into Bitcoin transactions. We can therefore say that while Bitcoin is poor in features, it is exactly this limitation that serves the property of security.

Ethereum and smart contracts

When trying to enable more use cases than simply receiving, storing, and sending Bitcoin, moving off-chain (moving away from the decentralized processing and storing of data) was not an option for the emerging blockchain community. Thus, in 2013, five years after the birth of Bitcoin, a group of visionaries around Vitalik Buterin created Ethereum. Like Bitcoin, Ethereum is a blockchain. Its native digital currency Ether is also scarce, but offers much more flexibility upon which developers can build. Ethereum is the world's leading programmable blockchain with approximately 200,000 developers1 and thousands of available applications. Ethereum's main programming language, Solidity, is turing-complete, i.e. it can implement any computational logic. Ethereum introduces the concept of so-called smart contracts. Smart contracts are programs that automatically execute transactions on the blockchain according to previously determined terms and conditions. They are relatively inefficient (in terms of latency and throughput) compared to centralized computing, because, like simple blockchain transactions, smart contracts are executed in a decentralized manner. That said, their strength stems from a high level of security and transparency. Anyone can potentially verify the results. Because of their decentralized nature, a set of interacting smart contracts are also called decentralized applications (dApps). In contrast to smart contracts, traditional banking software is neither visible nor understandable for the bank's customer. The user has to trust that companies' programs do what they promise to do. In contrast, no person, state, or company has to be trusted in smart contracts, because the code is publicly visible: copied thousands of times in public ledgers, which together form the blockchain. But, we want to be fair and note that only few users have the skills and resources to seriously evaluate smart contract code themselves. Similar to the traditional financial system, users usually end up trusting certain institutions or people such as auditors or experts.

Looking at the development of blockchain technology from Bitcoin to Ethereum, one can conclu- de that Ethereum adopted important aspects of Bitcoin, but expanded it by enabling computa- tional logic on top of it. If Bitcoin was poor in features, Ethereum is rich in them.

3 Building financial services bottom-up

In this chapter we explore how an alternative financial system can be built on the basis of smart contracts. We start at the very bottom with financial Lego bricks, the smallest units of DeFi, and ultimately look at the entire Lego house, an ecosystem of decentralized services.

Financial primitives: core financial functions coded into smart contracts

Smart contracts are very flexible and offer solutions for industries such as energy, logistics, healthcare, and in particular, the financial sector. Here, smart contracts can enable simple functions such as payment (stablecoin) and credit (lending/borrowing), as well as more complex functions such as derivatives (leverage, swaps) and trading with crypto assets (decentralized exchanges) – fully automated and decentralized without any intermediaries.

Decentralized applications that are based on a set of interacting smart contracts and serve these basic financial functions are referred to as financial primitives. Already today, financial primitives can incorporate functions like payment, lending & borrowing, trading, wealth management, derivatives, insurance and probably many more. While most of the DeFi applications are still analogous to existing financial products from the established financial world, one can expect entirely new DeFi use cases to emerge in the future. In theory, everything that is programmable is imaginable.

Financial primitives are the backbone of DeFi. A number of financial primitives build an ecosystem of interoperable services, i.e. the DeFi ecosystem. You can think of them as Lego bricks that can be plugged together with other Lego bricks as desired.

Building an entirely new financial system – the DeFi ecosystem and its architecture

Obviously, we are still at the very beginning of the development of DeFi, but it is impressive what has already been created in such a short time. Ethereum was only developed in 2013 and went live in 2015. The long-term vision of DeFi is to connect these »Lego bricks« in order to build a Lego house, a fully-functioning and fully-automated trustless financial system. We believe that the real advantages of DeFi lie in the intelligent combination of modularized financial primitives.

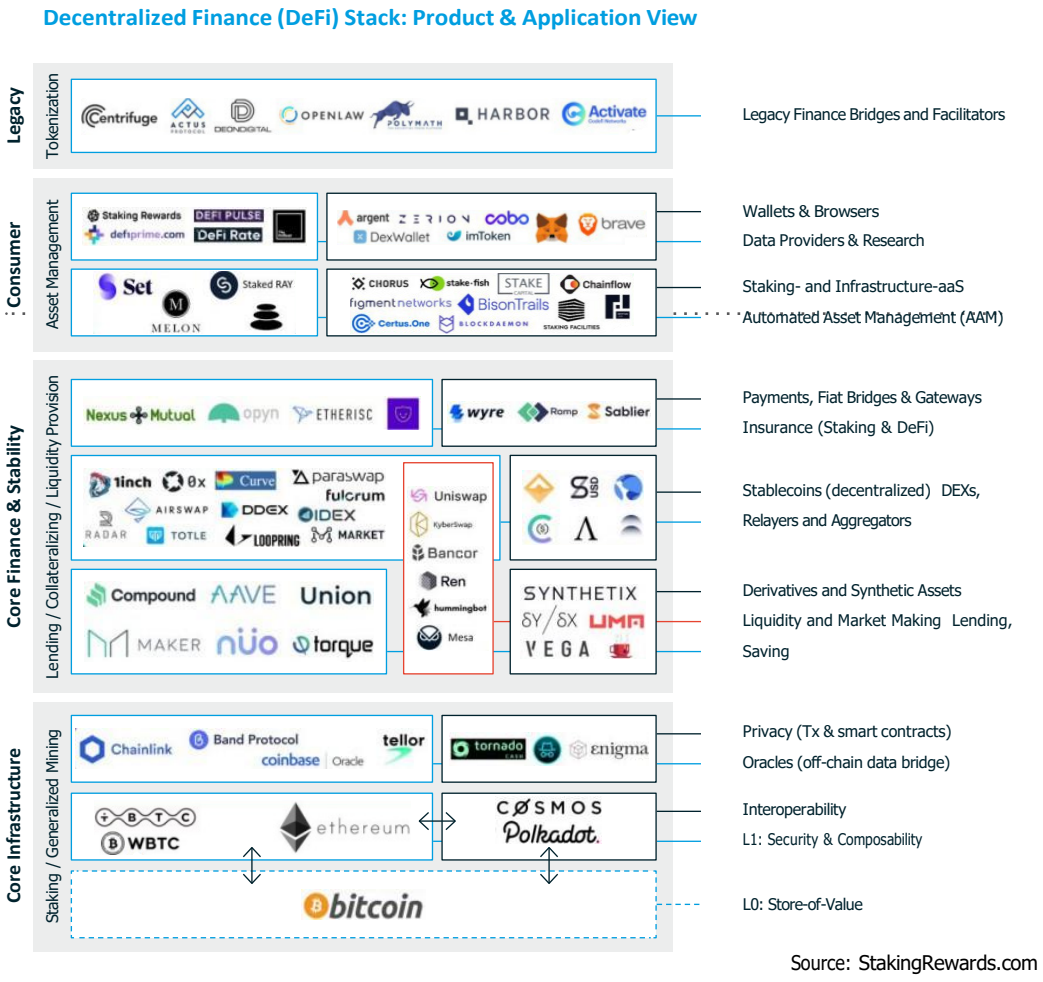

Figure 1: Decentralized Finance (DeFi) Stack: Product & Application View

While we only take a closer look at three DeFi protocols (Maker, Compound, and Uniswap) in our whitepaper, this diagram shows impressively the variety of different DeFi protocols that are currently being developed.

In DeFi, the blockchain (in this case called layer 0) provides the trust and security level. Above this layer 0 is layer 1: where basic financial functions such as a decentralized stablecoin for payments in the DeFi ecosystem are built (e.g. DAI and the MakerDAO-protocol, see chapter 4). The next level (layer 2) provides users with slightly more complex functions like lending/borrowing (e.g. Compound) and trading assets. This is followed by layer 3 and more sophisticated financial services built in dApps (e.g. decentralized exchanges (dEx) like Uniswap or prediction markets like Augur). Finally, on the aggregation layer 4, user friendly dApps combine different functions and build a service similar to what we know from today's banking apps: storing and sending money, investing in assets, borrowing against these assets (leverage trading), etc.

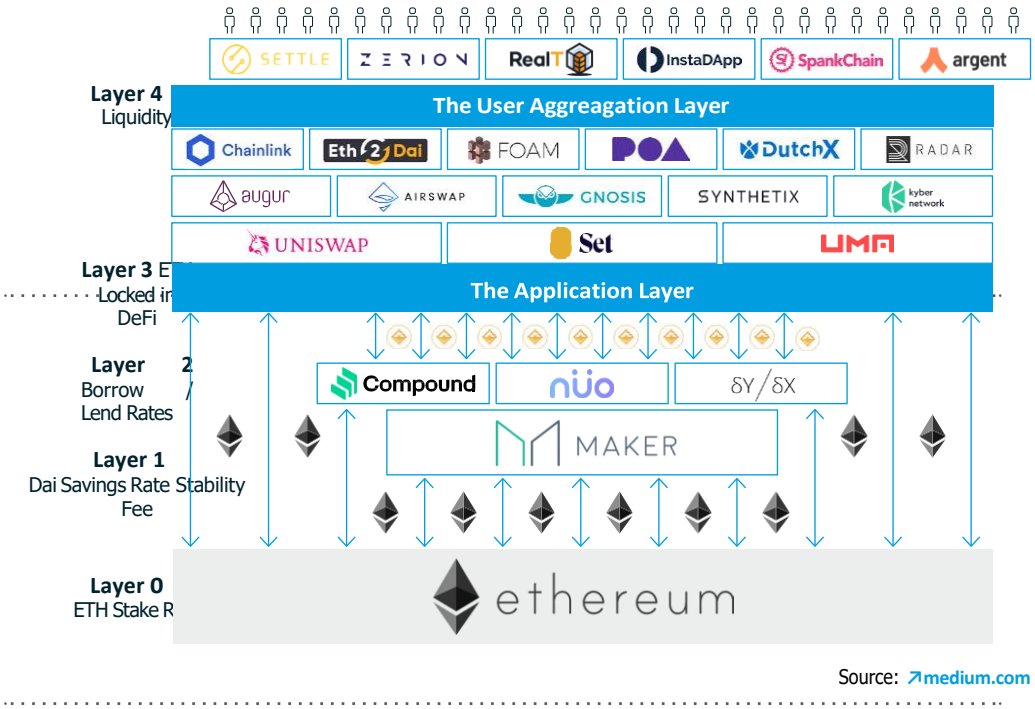

Figure 2: Decentralized Finance (DeFi) Stack: Product & Application View

This diagram illustrates how different DeFi protocols can be linked together and built on top of each other. Together, the various Lego bricks (DeFi protocols) create the DeFi ecosystem.

DeFi's vision and differences to Wall Street

DeFi wants to enable an alternative financial system that is built bottom-up, completely decentralized, censorship-free, low-fee, fully-automated, and without counterparty risk.

DeFi is, just like Ethereum and Bitcoin, permissionless, in that anyone can contribute code and use these open source protocols no matter their social status or country of origin. This is notably different from the regular banking system, where these two factors often determine and possibly limit one's chances to be served. DeFi democratizes financial services, especially those like individualized derivatives that can usually only be executed by large institutions. In DeFi, these derivatives have much smaller face values than in the traditional financial markets.

One might ask, with all this rebuilding of already existing financial products, what is the difference between DeFi and the established financial system? In DeFi, not only is every decentralized application (dApp) open source, but every single transaction is transparent. This is also true for dApps on higher aggregation levels. In contrast to this, Wall Street seems to be a black box where the user has to trust that these institutions do what they claim to do. Obviously, high compliance standards as well as strict regulation and supervision by state authorities like SEC, EBA, BaFin and FCA ensure financial stability, consumer protection, or fraud prevention. Centralized systems (financial services companies) are undeniably highly efficient.

Nevertheless, custo- mers have much less transparency on how their bank uses their money compared to open source and decentralized DeFi applications.

In conclusion, if Bitcoin is a modern, digital and decentralized alternative for transacting and storing value, DeFi is a modern, digital and decentralized alternative financial system as a whole. After this short and abstract introduction to DeFi, let's take a closer look at real-world DeFi applications

4 DeFi real-world examples

Throughout the illustration of three of the most prominent DeFi applications, it is crucial to keep in mind that the technology is still nascent and in a constant state of evolution. If we were to write this paper in two years, we would possibly be covering very different projects.

Financial primitive	Goal	Example in this paper
Stablecoin	Providing a stable digital asset	Maker
Borrowing/Lending	Providing the possibility to earn interest on unused assets	Compound
Exchange	Providing the possibility to swap two digital assets	Uniswap

Maker – Stablecoin

Maker is a stablecoin project. The programmable Maker stablecoin called DAI, that is pegged to the USD (1 DAI = 1 USD), is generated when a user sends Ether as collateral in a Maker smart contract and takes DAI out of it (»borrows DAI against his collateral«). In order to ensure price stability, the created DAI must always be secured with at least 150% collateral (Ether). For example, if Alice sends 150 USD worth of Ether into a Maker smart contract, she could withdraw up to 100 DAI worth 100 USD. This 100 DAI runs on the Ethereum blockchain, and can thus be moved anywhere in the DeFi ecosystem. If the price of the collateral falls below this limit of 150% for the created DAI, liquidation is automatically triggered and Alice's Ether deposited as collateral is sold at an auction. But how does this auction work out? Unfortunately for Alice, not only will Ether worth 100 DAI (equals 100 USD) be sold, but Alice also has to pay a 3% discount for the auction and an additional penalty of 13%. The discount of 3% is built into the auction in order to attract buyers for the Ether in auction. In addition to that, Alice pays a 13% penalty for not ensuring a sufficient collateralization of her DAI.

In the end, Alice is still left with 134 USD of her original 150 USD in Ether. She lost 3 USD through the auction discount and 13 USD through the penalty. Because she still holds 100 DAI, only 34 USD of her Ether collateral, which was originally worth 150 USD, will be paid back in Ether to Alice. In the end, she owns 100 DAI (equals 100 USD) and Ether worth 34 USD, so from the original 150 USD she has lost 16 USD. In order to avoid this loss through liquidation, Alice will make sure in the future she always has a higher collateralization in her Maker contract, e.g. 300% instead of only 150%. The DAI being used in the auction to buy the collateral (Ether) is destroyed (»burnt«) in order to not inflate the DAI supply. This also ensures that all existing DAI is always at least collateralized with more than 150% of value.

You may ask why Alice should lock her Ether in a Maker contract to pull out DAI. The answer is fairly simple: Alice could use her DAI for everything, from exchanging it to USD or EUR, to buying a house (and thus staying long in Ether while shorting USD or EUR respectively), to using it in the DeFi ecosystem to buy more Ether at a dEx (decentralized exchange, we come to that later) in order to leverage her exposure to the Ether price. She could also lend her DAI at a lending market place like Compound (next example) and earn interest on it. And she can do all this without selling her Ether.

Unlike centralized stablecoins like Tether, DAI is decentralized and does not rely on any compa- ny that could go bankrupt or could manipulate the system. Maker is not the only decentralized stablecoin project, though it is currently the most relevant and widely used. Many decentralized applications require a governance structure, for example to vote on configurations, or, in the case of Maker, to vote on the stability fee which users have to pay if they borrow DAI.

Compound – Lending and borrowing crypto assets

Imagine Alice bought Ether (ETH) for 1,000 USD at the beginning of 2017. As the price of Ether in January 2017 was around 10 USD, she got 100 Ether for it. This 100 Ether is worth about 20,000 USD in May 2020. Alice continues to believe that the price of Ether will rise, because, among other things, the innovations in decentralized finance will attract many new users to the Ethereum blockchain, causing increasing transaction fees and a value increase for Ether. At the same time, however, she would like to use another token, for example the REP token from the prediction market Augur. Alice could put 100 Ether as collateral in a smart contract of the lending and borrowing platform Compound and borrow REP. If Alice chooses a high collateralization ratio, the risk of liquidation and thus a partial loss of her Ether are significantly minimized and, while still holding her ETH, she can make use of the REP token. Alice could also, as in our Maker example, borrow DAI, convert it into a fiat currency (USD or EUR) and book a flight to Spain for her sister's wedding. She can do all this without selling her Ether, maintaining full control over her assets at all times and continueing to participate in the price changes of Ether.

Users can use the Compound protocol not only to borrow crypto assets, but also to lend them. If they borrow crypto assets, they have to pay interest, whereas if they lend them, they receive interest. When borrowing, collateral must always be deposited with a collateralization rate of higher than 100%, similar to the ratio of the Maker protocol. Every token on Compound has a dynamic interest rate that is determined in real time according to supply and demand. The interest is not simply credited once a year or monthly (compared to bank interests), but always at the time of a new Ethereum block, i.e. approximately every 15 seconds (»payment streaming«). Loans on Compound have unlimited duration. Similar to Maker, Compound also has a liquidation penalty. However, it is only 5% compared to Maker’s 13%. Other borrowing and lending platforms include dYdX and Dharma.

On 16th of June 2020 Compound released the COMP token. Holders of this so called governance token can propose and vote on changes to the Compound protocol. A few days after the release of the token, the price soared to astronomical 427 USD per token2, but later fell to 170 USD in July. The trading of governance token (COMP token for Compound protocol, MKR token for Maker protocol) is about to become an interesting investment opportunity for some tech savvy traders.

Uniswap

Uniswap is a completely decentralized exchange for ETH and other tokens that are issued on the Ethereum blockchain, for example Compound's COMP token. Uniswap provides two main use cases: users can provide liquidity for others who want to exchange tokens or they can exchange tokens against each other. If you provide liquidity, you earn a commission fee of all trades being made by traders. In the following we will take a closer look at the two use cases:

1. Bob wants to provide liquidity for a so-called liquidity pool. First, he has to decide on a specific Ethereum-based token for which he wants to provide liquidity. Bob opts for the COMP token. If Bob now wants to provide COMP tokens worth 100 USD to the COMP liquidity pool, he must also provide ETH to the same amount, i.e. also ETH worth 100 USD. Bob would then have invested 200 USD. All users who provide liquidity for his pool would then earn 0.3% of the commission fee on every trade that takes place in the ETH-COMP currency pair. How much Bob earns exactly on all commissions in the ETH-COMP pool depends on his share of the total ETH-COMP liquidity pool. Bob can withdraw his liquidity from the pool at any time.

2. Next, Bob would like to swap ETH for DAI. This is very simple: Bob selects the appropriate currency pair and is directly offered the price. With one click Bob exchanges the tokens, paying a commission fee of 0.3%. He would pay twice the commission fee (0.6%) if he were to exchange DAI for COMP, because Uniswap performs two swaps in the background: first DAI for ETH, and then ETH for COMP. Now, imagine that Bob accidentally enters 1,000 ETH instead of 1 ETH, and the price for the swap suddenly becomes much more expensive. To understand why this is the case, we must to take a closer look into Uniswap's pricing mechanism.

Pricing with Uniswap

With Uniswap, price determination does not work via an order book and active market making, as is the case with centralized exchanges, but fully automatically via a formula called Automa- ted Money Making (AMM) Curve Function:

The curve displayed here shows all possible prices for the currency pair A-B, for example REP-ETH, with REP being another Ethereum-based token. If a swap of 10 ETH against 139 REP takes place, the share of REP in the liquidity pool is reduced by 139, but the share of ETH increases by 10. Since k in the equation x * y = k always remains the same, the price of this currency pair in the Uniswap exchange now changes. But not for long, because arbitrage traders will use price differences between exchanges, whether centralized or decentralized, at any time, and the price difference between the exchanges will quickly decrease, especially in currency pairs with high liquidity, i.e. big liquidity pools on Uniswap. In order to keep this white paper as concise as possible, we won't dive deeper in the pricing mechanism of Uniswap, however we recommend the interested reader to play with the ↗**price mechanics** or find a more detailed explanation of the ↗**Automated Market Making formula**.

Uniswap does not aim to replace centralized exchanges, but to complement them. Its price correctness is based on arbitrageurs. So-called whale trades (very, very large sums of money traded) will probably not happen in the next few months on Uniswap, and certainly not in currency pairs with low liquidity, as it is highly likely that they would have to pay more for their tokens than on other exchanges. Uniswap will, however, contribute to the efficiency of the pricing of the entire crypto-market as it is another exchange that functions completely decentralized and is therefore less vulnerable to manipulation.

Another exciting advantage of Uniswap is that every user is able to open a new swap pair, i.e. a new Uniswap exchange. For any new token that is compatible with the Ethereum blockchain, this quickly offers new trading possibilities.

5 DeFi risks and challenges

As mentioned previously, DeFi is still a nascent technology and the real-time adoption lags far behind the promising theory. In order to gain the trust of people and institutions beyond the crypto-native community, DeFi applications have to overcome some major obstacles and risks. While we tried to identify and present the most important risks in this chapter, it is essential to note that those are inextricably linked and affect each other.

Technical Risks

By design, false or fraudulent transactions are irreversible on the blockchain. DeFi relies heavily on the integrity of smart contracts and the underlying blockchain protocol. Any failure in the code could lead to a hack and to massive losses for users of a decentralized application. It is almost impossible to code error free, particularly if one has to take into account future developments of the blockchain protocol. Additionally, the detection of bugs in smart contracts is quite a complicated endeavor, partly due to the novelty of the technology and missing standardized procedures.

Consequently, there have been a wide range of DeFi hacks where several million USD of value have been stolen and/or lost in different projects3. Potential remedies for code bugs and technical failures could be third party audits and insurance schemes, regulation (see regulation subchapter) in the form of necessary risk management procedures, capital buffers, and consumer protection. Alternatively, transparent and formalized processes of »good governance« within the DeFi protocols, which can quickly freeze the smart contract, update the code, or even undo certain transactions in extreme cases, such as the DAO fork refund 20184.

Apart from risks regarding smart contract bugs and inaccuracies, technical risks regarding the underlying blockchain protocol (layer 0) also have to be taken seriously. Nearly all relevant DeFi projects are built on top of the Ethereum blockchain. In times of high usage, Ethereum has experienced a few clogging issues on its blockchain. If the network gets congested, a transaction can remain in a pending state, which ultimately results in market inefficiency and information delays. Those technical scalability problems are closely related to liquidity risks (see liquidity subchapter). Given the current bottlenecks in terms of throughput, it is highly questionable whether DeFi is viable on Ethereum, especially if Ethereum experiences a further user base growth. In short, DeFi is thus highly dependent on a successful Ethereum 2.0 update, which could solve these technical issues, but is expected to take at least several more years5.

Other smart contracts offering blockchain platforms (EOS, Tezos etc.) could also take over Ethereum's leading role in the DeFi space, but currently face other problems such as insufficient decentralization (see centralization subchapter) or a missing developer/community base. Part of the reason why Ethereum is currently the leading platform is because its high usage leads to high Ether and Gas prices which attract miners that in turn guarantee a high security for the network. Despite its challenges (see e.g. the liquidity risk chapter), Ethereum is today the most decentralized and secure smart contract blockchain.

Usability risk

A risk, or better, a major weak point closely related to the technical implementation, is the usability or user experience of DeFi protocols that are often complicated, unintuitive, and designed for crypto-native users. DeFi projects have struggled to gain traction beyond those that are inherently familiar with Ethereum. Many products require users to handle multiple tokens within their own, non-custodial wallets. Realistically, it is still way too early for the mainstream audience to risk their money in this complicated and unchartered territory. Once the technical and regulatory risks are addressed, the UX of DeFi products will certainly be one of the top priorities for developers. Looking back to the mass adoption of the internet, where first applica- tions were anything but »easy to use« compared to today's social media platforms or intuitive brokerage services, one can be hopeful that DeFi will overcome this UX challenge.

Centralization risks

Many DeFi applications were kick-started by a certain team or company and are far from being truly decentralized, although, once established, they generally aim towards decentralizing governance and decision making. As long as an application is semi-centralized (with funds transiting through an intermediary or with an intermediary being able to freeze funds), counterparty risk exists, and the intermediary that has control over the assets may use the funds maliciously.

For example, Compound, the second most prominent DeFi lending protocol, was designed with the ability to be upgraded in place by a central administrator. Only recently, the platform launched its COMP token and started decentralizing its governance, openly stating that this shift would be conducted over a period of time6. As of today, despite the word »decentralized«, most of the projects have master keys for the developers that allow them to not only shut down or disable the decentralized App, but also to proceed easily with upgrades and provide an emergency shut off in case of a technical problem. As the code and the decentralized governance models become more battle-tested, we expect DeFi projects to gradually get more decentralized and give up these central backdoors.

On the other hand, once these DeFi projects grow in terms of user base and assets locked in, they will definitely fall under stronger regulatory scrutiny and a financial supervisory. Financial regulation will, without a doubt, require some degree of responsibility and competent counterpart, which could in turn engender a move back towards a more central administration of DeFi projects. A hint in this direction is the renunciation of the Libra association to pursue a future permissionless system in its Libra 2.0 Update7.

A scenario in which DeFi projects are governed in a truly decentralized manner is currently difficult to imagine. How are compliance and regulatory requirements addressed by a decentralized form of governance? What if the majority of token holders in a decentralized decision making model simply don't vote for compliance updates or financial anti-money-laundering (AML) requirements? Both the regulator as well as the DeFi sector have yet to come up with viable and sustainable solutions in that regard. Since many DeFi supporters nowadays still refuse the idea of clear regulatory responsibilities in favour of concepts around security/compliance by design, we expect these incompatible perceptions of responsibility and regulation to further clash in the coming years.

Furthermore, most DeFi Apps currently rely on oracles, third party services that send and verify real world data and submit this information to smart contracts. Generally, the centralisation problem raises the following question: if you (today or in the future) rely in any way on third parties, then why not just rely on trusted and regulated third parties to manage your money, while also offering valuable things like a help number and recourse in case of erroneous transactions?

Future DeFi governance models as well as regulatory approaches will show whether DeFi will be able to overcome the central risk and challenge of (de-)centralization.

Liquidity risks

Liquidity is crucial for efficient pricing in the financial industry. Currently, liquidity in DeFi protocols is largely outpaced by central alternatives with many low-fee liquidity providers that stabili- ze traditional finance. The liquidity risk is closely related to technical risks, i.e. the aforementio- ned technical scalability and congestion issues on the Ethereum platform. In times of crisis, the Ethereum network (Bitcoin as well) becomes so congested that arbitrageurs and liquidity providers cannot keep prices in line across venues, causing massive dislocation on individual exchanges, which then triggers uncertainty and the markets to drop.

On Tuesday, March 12, crypto markets dropped nearly 40%, coinciding with a global stock market decline due to the Covid-19 virus. When volatility picks up and markets drop, a few things happen concurrently: liquidations in DeFi projects such as in Maker's smart contracts accelerate, arbitrageurs that don't have enough capital on each venue begin shuttling assets between the exchanges in order to arbitrage the price discrepancies, and demand for blockspace explodes upwards. Transaction fees on Ethereum skyrocket, and transactions don't get included in a block for minutes, or even hours.

At the same time, as prices collapse, miners start turning off their machines because mining revenues fall below the cost of electricity, which in turn further slows the rate at which new blocks are produced, increasing latency and decreasing aggregate throughput8.

On this day, not only the crypto market suffered this downward cascade, but DeFi particularly failed and suffered. Maker, the largest DeFi protocol and the foundation on which much of the rest of DeFi is built, nearly imploded. As a result of crypto markets crashing, many Collateralized Debt Positions (smart contracts holding the collateral) were liquidated, but as the Ethereum network congested, many liquidation transactions were not included in blocks. Therefore, as far as the Maker protocol was concerned, no one was bidding in the collateral auctions. Someone realized that by just increasing transaction prices, she would be the only auction participant, and could therefore bid as low as 0 USD for the collateralized Ether. So in a Maker auction she bid $0 for $8M worth of ETH collateral (paying an unusually high transaction fee), and got it.

Additionally, the software that powers the Maker oracles was not configured to run in a highly congested network. Many of the oracles simply stopped sending prices to the Maker contracts. Had the oracles conveyed that the Ether price had dipped down to $88 around 7pm on the 12th, many more of these collateral debt positions holding the Ether would have been liquidated, and Maker could have become insolvent, with dramatic consequences on the stability of »stablecoin« DAI and other DeFi protocols, including Compound or Lendf.me that use DAI as collateral for loans. As such, the interdependencies between DeFi protocols, and particularly the current reliance on the DAI stablecoin, represent a potential systemic risk for the whole DeFi space.

As of today, the Ethereum network as well as arbitrageurs and liquidity providers in the crypto space are not yet able to provide global-scale capital markets activity and liquidity. A potential remedy for future liquidity shocks could be the Ethereum 2.0 Update that improves throughput and latency, or also more professional and powerful arbitrageurs and liquidity providers that have the necessary resources on all major crypto exchanges.9

Regulation risk

Decentralized projects operate without a license in most jurisdictions, regardless of where the end-user is based. With regards to taxation, the handling of DeFi assets is also not clearly outlined in most jurisdictions. Today, DeFi activity is about 1% of the total crypto market activity, which itself is tiny in comparison with global financial markets. In the same way that regulators around the world are currently addressing regulatory questions regarding crypto-assets – such as establishing new license regimes for crypto custody like in Germany10 – DeFi assets and products will certainly fall under stronger regulatory scrutiny given that the user base and locked-in-assets will further grow. Financial regulation will necessarily require some kind of responsible counterpart, which makes a truly decentralized governance and decision making process for DeFi products not yet imaginable. The Libra association, renouncing to move towards a fully permissionless system in view of the political and regulatory pressure, seems to support this ideas.On the other hand, if DeFi projects try to fully satisfy financial supervisors by establishing responsible counterparts, they counter their core DeFi belief of true decentralization and disin- termediation. One possible solution to this dilemma might be a new way of supervising and regulating financial risks, called »embedded supervision« by the Bank for International Settle- ment11. This paradigm shift of regulation would allow compliance with regulatory goals to be automatically monitored by financial authorities by reading the market's ledger as an active DeFi infrastructure participant, including the ability of intervening or shutting down a project. This would reduce the need for DeFi projects to actively collect, verify, and deliver data or to interve- ne with compliance occurrences (KYC, AML etc.) themselves. Such a paradigm shift in the future would completely turn financial regulation upside down and cannot be expected to be realized in the short or mid-term.

6 Outlook

Overall, the blockchain-powered space of Decentralized Finance is clearly still in its very early days. In 2020, the monthly number of DeFi users ranged between 40,000 – 60,000, with 90% using decentralized exchanges12. Even compared to central crypto-exchanges with several hundred thousand daily active users each, that figure looks tiny, not to mention applications of our well-known and established traditional financial system. For now, DeFi remains a visionary side-ecosystem in the blockchain space.

Nevertheless, it is also clear that DeFi offers an immense disruptive potential and a very compelling value proposition whereby individuals and institutions make use of broader financial applications without the need for trusted intermediaries. Andreesen Horowitz, one of the most renowned and prestigious venture capital funds in the world, just recently launched a second $515 Million crypto fund to invest in crypto networks and businesses, highlighting DeFi as one focus area. »With programmable trust, scarcity, and value as new building blocks, DeFi opens the components of finance to the same recombination and experimentation that makes open-source software so powerful.«13

On its road to mass adoption and the realization of its ambitious promises, DeFi still has to overcome major obstacles. Technical aspects regarding smart contracts, the underlying Blockchain protocol, and the usability of most DeFi applications currently hinder wider user adoption and growth. Regulatory considerations, which will certainly emerge once DeFi becomes financially relevant, will pose currently insurmountable requirements on those decentralized projects. And finally, the DeFi ecosystem still has to demonstrate how to reach its true goal of decentralization and decentralized governance, not least in times of (liquidity) crises.

There is still a long way to go for DeFi, and none of these sizable challenges will be completely solved in the coming years. Nonetheless, we firmly believe that in the long term, a maturing DeFi ecosystem will, together with political stakeholders, regulatory supervisors, and the traditional financial sector, forge the necessary conditions and frameworks that allow it to realize its full potential. Understanding, cooperation, and integration between these relevant players are key towards that goal, and we are eager to further create and strengthen these ties within our cross-industry platforms.