Group Assignment:

Decentralized Equity Funding

Group 7:

Gabriele GRIGNANI, Sid LAMICHHANE, Giacomo MASSINI,
Matteo RIGHI, Emanuele SORGENTE

30TH NOVEMBER 2022

EPFL

Abstract

The initial public offering (IPO) is a necessary but often difficult step for any company which aims to become successful. By putting up shares on the stock market, the company is able to secure funding for future development. However, the process of doing an IPO is long, expensive and difficult. On the other side, certain potential investors can have difficulty in opening a stock portfolio to invest in shares, notably for investors from developing countries. This paper proposes a new decentralized finance (DeFi) protocol called decentralized equity funding (DEF) to address these problems.

Broadly, DEF functions as follows: companies can create Equity Tokens (ETs), which are put up for sale. Just like with stock shares, ETs give the holder the right to receive dividends and to make decisions on the company. The protocol funds itself by charging a fee on the sale of ETs. A governance token gDEF is distributed when users buy ETs; the gDEF token allows users to take part in the governance of the token.

The DEF protocol has some intrinsic limitations. Notably, there is little which can be done to prevent malicious users from selling tokens without an underlying company, and then keeping all the acquired liquidity. Furthermore, any DeFi protocol is vulnerable to cyber-attacks. There are no simple fixes to these problems, only partial solutions which mitigate the risks; going forward, it will be important to keep the protocol updated to limit new vulnerabilities.

1   Introduction

1.1   Context

Financial intermediation enables investors and companies to find each other in the easiest way; however, financial intermediaries don't always act in the best interests of clients, and can sometimes pursue their own personal goals. An important role of financial institutions is to help different players build trust in the financial markets and to offer the best deals to minimize transaction costs. Even though in the past these functions have been crucial, in the current day many investors are starting to feel a need for change [1]. The digital revolution of the last two decades has brought changes in all domains, and finance is no exception: starting from 2009, financial technology (FinTech) companies have succeeded in replacing financial intermediaries for certain operations [1], and, for the first time, large banks have been less needed. This business model uses technology to make financial operations automated; some examples could be peer-to-peer services and platforms such as PayPal and Revolut. The goal of these companies is to simplify the transfer of money between individuals without the intervention of a central institution [2]. However, FinTech companies cannot remove financial institutions from the picture on their own because, even if the operations are facilitated, there is still a third party which is involved in the transactions. This is where blockchains and DeFi come into play.

DeFi protocols can make transactions easier and more secure. In the context of DeFi, the concept of trust has changed: it is no longer an agreement between parties or institutions, but something built through a distributed network. This idea has led to the creation of decentralized platforms, where, notably, new companies have the chance to create their own financial system without the involvement of intermediaries such as investment banks. Decentralized Equity Funding (DEF) is a protocol created to be part of the Decentralized Finance (DeFi) space and to answer the requirements of both companies and investors. Through DEF, any company will be able to issue a non-fungible token (NFT) on their equity. It is important to distinguish these tokens from cryptocurrencies: NFTs cannot be duplicated or exchanged with other NFTs, which guarantees the companies that they provide a unique product that cannot be crafted otherwise. These products, hereafter referred to as Equity Tokens (ET), share some similarities with common stocks: possibility of exchange, giving rights over the company and owning a share of it [3]. Nevertheless, they have one important difference: all the information regarding the agreement between equity holders and the company will be stored on a blockchain rather than on a public register. This difference is fundamental: investors are increasingly concerned with what happens to their data and some of them might not be happy with their data being stored on a centralized exchange; indeed, bloclchain technology makes it is harder for hackers to steal funds in DeFi compared to in banks, where money can just be sent to another account. Moreover banks can be more sensitive to cyberattacks and fraud. [1]
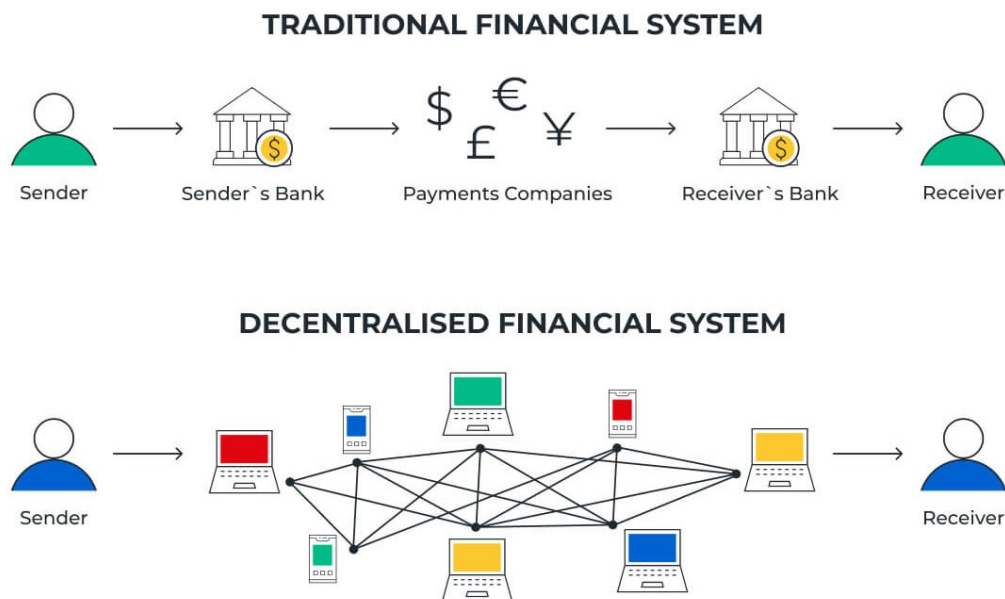
Figure 1: Comparison Traditional - DeFi
Image source: Up tech

1.2 Motivation

Investors in ETs get many different and flexible control rights over the company, notably voting. For investors who own a significant share of the company, this right is very important, as then they can influence decisions like M&A, composition of the board of directors, policy changes, etc. However, the DEF protocol is targeted mainly at small companies and start-ups which are looking for funding. In general, start-ups take several years to reach a positive cashflow: they lose money at a constant rate for the first few years while the product is developed, and stay afloat only thanks to investors (angels, VC companies, family, etc.); once the product starts to sell, they are able to grow and turn a profit; it is only once they become sufficiently profitable that they can do an IPO or M&A. The rule of thumb is that the company must be worth at least 100 Million USD before they can go public on the market. Moreover, 92% of startups go bankrupt within 3 years. DEF aims to avoid all these apparently necessary steps in the life-cycle of a company by giving them the chance to go public while their capital is still low, the revenues are low and few people are aware of the project. This way, startups can gain access to funding in a more direct way, as long as there are investors who believe in the project and are willing to invest in it.

It has been observed that the most important financial institutions in the market have

a tendency to create monopolies around them, and this can generate a big surplus on transaction costs. DEF guarantees investors smaller transaction costs, as it will be themselves that set the charging fee and it will be much more difficult for a single participant to store enough capital to create a monopoly. Moreover, this protocol guarantees companies much more flexibility than going public in the stock market, as all the benefits and policies given by Equity Tokens will be established by the company itself and not by a third party.

Recently, there has been a renewed interest in sustainability in the financial world [4]. This is not an easy topic, as profits tend to be a higher priority than issues of sustainability. Financial institutions, in particular, pose problems of inclusivity (which is part of the social dimension in sustainability issues), notably as concerns people from developing countries. One of the problems that DEF is aiming to solve is to be more inclusive and sustainable by creating an asset that anyone can issue and anyone can buy, from any part of the world. Note that this principle is in contrast with what the idea behind centralized exchanges, where only specific countries can trade assets in specific currencies. DEF could help transition to a borderless and sustainable financial system, where everyone can become an entrepreneur or an investor.
In addition, DeFi increases the transparency of all transactions, through the use of blockchain technology, which discourages opportunistic players from damaging the system.

1.3   DAO

By the explanation of the DEF protocol it emerges that every company that issues Equity Tokens becomes similar to a Decentralized Autonomous Organization (DAO). The definition of DAO is quite broad, but all DAOs have some common features: they have a decentralized governance, whose rules are decided amongst the people who are coordinating it, and they are deployed on a public blockchain exploiting smart contract technologies. It is important to note that the term DAO does not refer to a specific kind of business, but rather it is an idea which can be used in many different applications. Hereafter, the term DAO is used to describe any entity which issues Equity Tokens. This concept could radically change the economics system as we know it, since it is a framework that may lead to a more democratic and inclusive kind of governance, which, as it is mentioned above, is the ultimate goal of the protocol. There are many open discussions in the blockchains academia about what can be classified as DAOs or what being a DAO implies, and many think that a DAO cannot be interpreted as a legal entity, and this has significant implications in the compliance of law [5]; for simplicity, we will disregard these issues in this paper.

1.4   Participants

DEF presents several advantages both for companies and for investors. For companies, DEF provides an attractive alternative to conventional stock IPO's. A company's initial public offering or IPO is the first moment when shares of the company are available for purchase. For growing companies, selling shares is a convenient way to raise capital, which can then be used for further expansion of the company. However, the procedure to do an IPO is not easy: firstly, the company needs to be accepted by an investment bank; next, they need to complete a long and expensive legal procedure to apply and, should they be accepted, to register with the stock exchange. In this way, the initial step will shut the door to a majority of companies looking for funding; and the long and expensive second step will discourage others. In addition, once the procedure is completed, the investment bank retains much of the control over the shares, notably on how many are to be issued and how much they should cost.
DEF provides a solution to the main shortcomings of the conventional stock IPO. This comes in three parts: firstly, DEF is open to all companies. Secondly, the procedure of doing an IPO over DEF is faster and less expensive, as it involves only writing a smart contract; in addition, this procedure does not require technical know-how, as smart contracts are generated automatically by DEF. Thirdly, once the IPO is finalized, the company owners have control over the shares, including their number and price.
DEF provides the additional benefit, compared to stock IPO's, that the shares are put up directly on the primary market, which opens the company to a broader range of potential investors.
Following this reasoning, DEF could be an attractive alternative to usual stock IPO's for certain companies looking for funding. We see two main categories of companies which might be interested in DEF: firstly, small companies or start-ups that have not been accepted by investment banks, or that do not have the resources or the time to undergo the procedure to do an IPO. Secondly, companies that want more control over their shares, and that wish to be independent from the banks.

DEF also provides several advantages for investors compared to the stock market. We see three main advantages:
Firstly, the stock market is not open to everyone. The stock market is open to a small number of large financial institutions, and investors invest through these institutions. Through this mechanism, investors have to approach one of these institutions and ask to open a portfolio. Often, it is necessary to have deposited a certain amount of capital with that institution to open a portfolio, which is not an option open to everyone. On the other hand, DEF is open to anyone with an internet connection. Thus, DEF might be interesting for investors who are not able to open a stock portfolio. Concretely, this is interesting especially for investors in developing countries, who usually would have difficulty in opening a stock portfolio, or might not be able to invest in the currency of their country. This feature is fundamental in our goal of ensuring an inclusive and fair investing space.
A second advantage of DEF for investors is that it gives access to a broader range of

companies. As mentioned above, companies listed on the stock exchange must first be accepted by an investment bank, whereas DEF accepts all companies. This way, investors on DEF have access to a broader range of companies. We see that this feature could be attractive to investors interested in riskier investments with small companies.

This system necessarily provides a fundamentally different offer to the investors: companies which do an IPO through an investment bank can provide investors with the stamp of approval from an investment bank which guarantees that they believe the company to be a good investment. As DEF has no comparable guarantee mechanism, investments are intrinsically more risky. However, while the selection process for a conventional IPO guarantees that all selected companies are reliable, it does not guarantee that all reliable companies are selected. We hope that DEF can be a solution for companies who "fall through the gaps", that is to say, companies which ultimately turn out to be profitable, but which were rejected for an IPO. From the point of view of investors, this could be interesting, as it would signify a higher profit on the investment.

On a more ideological level, the idea is to take the power away from the banks, and to give it to the people: this way, there is no fallible entity to determine who gets to do an IPO, only the decision of the people to buy or not to buy the shares. Note also that companies on DEF can choose to put up a collateral, which they lose if their offer turns out to be fraudulent (this is explained in section 2.2), which provides a minor form of guarantee. Thus, not all investments on DEF are very risky.

Finally, Equity Tokens purchased over DEF are more secure than stocks: whereas stocks ownership is listed on private ledgers which might be lost or damaged, Equity Tokens are stored on the blockchain, which necessarily makes them public and immutable. This provides advantages with respect to security, as this way the records cannot be tampered with.

2   DEF Protocol

2.1   Blockchain

The DEF protocol is built on top of Ethereum as it is the most popular blockchain both for developers and for users. Because of this, the Ethereum developers and its community have created many standards, like the popular ERC-721 [6], making the development of DEF faster and secure (see section 2.2). Ethereum is also a good choice from the perspective of ET holders, as it hosts many of the most popular NFT marketplaces which they can use to sell their ETs. Additionally, due to EVM compatibility, the code base of the Ethereum version of DEF does not need to be modified in order to be deployed on other popular blockchains like the Binance Smart Chain, Polygon or Solana.

2.2 Fundamentals

At its core, DEF simultaneously functions as an investment bank and as the primary market for ETs. As an investment bank, DEF gives companies the infrastructure to create their own personalised ET and thus go public. Technically, all ETs are of the same instance and thus have the same functions. However, during creation, the issuing company has to set up a unique name and a minting fee, making each ET unique to the company which issues it. Optionally, companies can further personalise their ET, for example by setting a royalty fee applied to secondary market transactions of ETs.
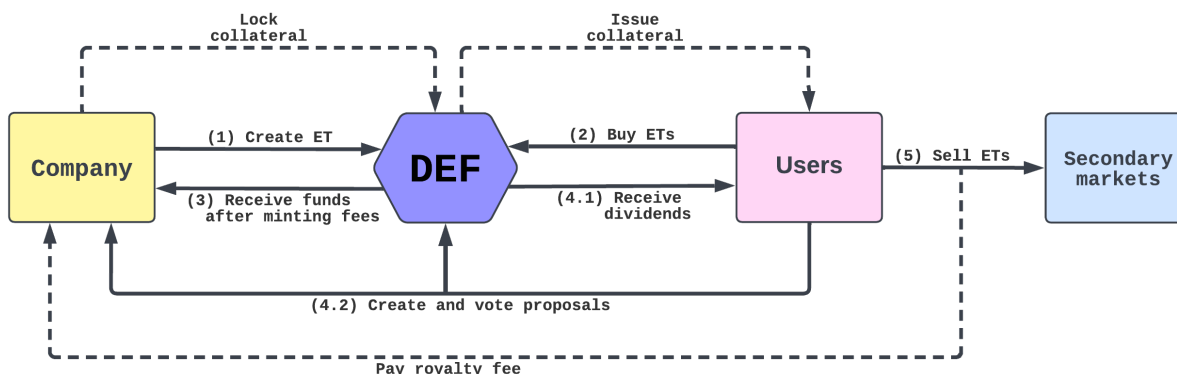

Figure 2: Diagram of DEF's functioning

As a primary market, DEF is where an individual can initially buy and thus mint ETs. The minting price is determined by the company itself, which gives the company control over the amount of capital that it wants to raise. Minting comes with a fee which is paid by the company issuing the ETs. Consequently, companies going public only pay the DEF protocol once their equity is actually sold.

Owning ETs gives the holder several privileges. One is the right to make proposals regarding the company which issued the ETs. Every proposal is discussed and voted on, giving DEF's public companies a DAO-like character. Another privilege for ET holders is their eligibility to receive dividends. There are two ways the protocol pays dividends: first, companies can set up their ET so that it automatically issues a dividend of a certain amount of ETH per ET to all ET holders at predetermined intervals, for example every financial quarter. Second, ET holders can make an official proposal for a dividend payment which needs to be accepted by the majority of ET holders. Since short-term ET holders are keen on getting their return-on-investment fast, it is in a public company's interest to attract and maintain a majority of long-term holders who instead will want to keep money within the company, instead of proposing dividend payments.

If ET holders do not wish to make use of the privileges of their ETs anymore, they can sell them on NFT marketplaces such as OpenSea, which can therefore be regarded as a

secondary market for ETs. During the creation of the ET, companies can opt for a royalty fee. Note that the fact of having a royalty fee or not will affect the attractiveness of the ET to potential investors, and should therefore be carefully considered by the company. Companies can also choose to implement a royalty fee after the ET has been created; for this, a proposal needs to be made and accepted by the majority of the ET holders. This way, the majority of the ET holders can penalize ET holders wishing to sell by increasing the royalty fee; this helps to ensure that ET holders aim to support the company, and discourages speculation.

The royalty fee can be implemented through ERC-2981 [7], a standard created to provide royalty payments information to enable universal support across NFT marketplaces. In particular, this standard creates an interface that provides the address of the recipient and the amount to pay given the sale price of the NFT. However, the main limitation of this method is that it does not enforce the use of royalties, as the marketplace can decide to just ignore the ERC-2981 interface when carrying out the sale transaction. To solve this, it could be possible to create a custom marketplace where ETs are traded, so that the protocol has full control on the sales and the relative royalty fees.

In order to make their ETs more desirable, companies can pay a collateral to the DEF protocol. Such collateral is paid out to ET holders in two cases: if the underlying company goes bankrupt, or if it fails to make the promised dividend payments it has manifested in its ET. It is up to a majority vote of ET holders to determine if bankruptcy occurs. However, bankruptcy can also be declared automatically by the DEF protocol. To do so, DEF makes use of the financial standing every public company on DEF has to publish for each fiscal quarter. This can additionally be regarded as a hurdle for malicious issuers of ETs. Nonetheless, DEF has as of now no influence on the correctness of the published financial standing. However, DEF believes in a future where all its companies' cashflow is on the Blockchain and thus can be audited. For some companies this is already the case since they are protocols on Blockchains. Once bankruptcy is determined, holders get their share of the locked collateral and all ETs are burned. As a result, a company should make sure that its ET holders regard it as more valuable than the collateral. This is for long-term investors really subjective compared to short-term ET holders only buying ETs to flip them on the secondary market. These people immediately vote for bankruptcy if the collateral is more ETH than the combined value of all issued ETs which is the product of ETs in circulation and the ETH price of the respective ET in the secondary market. Therefore, DEF's public companies should once more make sure that the majority of their ET holders believe in them for the long-run.

From the technical point of view, DEF is a single smart contract which produces personalised instances of the ET smart contract. This ET smart contract is an extension of the ERC-721 NFT standard and thus makes ETs easily tradeable as well as understandable for many. Besides the built-in ERC-721 functionalities, ETs are equipped with the following functions:

- Follow-On Public Offering to raise additional capital (i.e. increasing the amount of mintable ETs);

- Paying dividends to ET holders;
- Splitting equity, i.e. giving each holder a certain amount of ETs for each ET they hold, hence increasing the supply and decreasing the value per token;
- Making proposals and voting on them.

2.3 Revenue Model

To fund the development of DEF and its future updates, but also to attract new customers and to reward the governance token holders, it is necessary to implement a revenue model that allows the protocol to sustain itself. The main source of income comes from the initial minting of the ETs: a percentage of each payment is deducted by DEF before being sent to the company issuing the ETs.

This minting fee is then redistributed to three parties:

1. The development team, which will use the money to pay salaries and as an emergency fund for any urgent need;
2. The governance token (gDEF) holders as a reward for their help in managing the protocol;
3. The company that issued the token being sold, as a reward for having used the protocol and having an active market for their ETs.

The percentage of the fee and the way it is split and redistributed are decided by the governance of the protocol through the vote of proposals (see 2.4).

2.4 Governance

The DEF protocol is designed to behave as a DAO itself, and therefore it needs a governance structure to manage the smart contract and adapt its behavior to the needs of the users. To allow people to take part in the administration, a governance token called gDEF is created following the ERC-20 standard (fungible) [8]. gDEF tokens are minted and distributed to the users every time they buy an ET during the initial offering of a company, in a quantity proportional to the purchase made. The goal is to reward users for their participation in DEF.

The gDEF token then allows users to create and vote proposals that modify how the protocol operates. For example, it would be possible to change how the minting fees are redistributed between developers, gDEF holders and companies in order to shift the focus of the protocol and respectively incentivize new updates, more participation in the governance or attract new companies to the protocol. To avoid the exploitation of these mechanisms, such as completely removing fees redistribution to one or more parties, the developers can impose hard limits on the minimum or maximum values that these parameters can be set to.

The fundamental role of governance is to keep the protocol sustainable and profitable. Notably, the distribution mechanism of gDEF during minting seems to cause inflation of the token and therefore a constant decrease in its value. However, the fees redistribution to gDEF holders counterbalances this effect by indirectly increasing the value of the tokens as more money is given to the holders.

Let T be the total value of the gDEF tokens before the minting. Let P be the price to purchase a new ET during an initial offering. The governance of the protocol can define the values of the parameters $mint\_gDEF$, which expresses the value of minted gDEF tokens as a percentage of P, and fee_to_gov, which expresses the percentage of P redistributed to the governance (both parameters are between 0 and 1). These will in turn define $m = mint\_gDEF \cdot P$ and $f = fee\_to\_gov \cdot P$, which are respectively the value of minted gDEF given to the buyer and the fees amount that will be redistributed to the current gDEF holders.

As long as the holders receive rewards that are greater than the loss due to inflation, it will be profitable for them to not sell the tokens and the market value of the gDEF should either remain stable or increase as new users decide to buy more gDEF. At the same time, however, a larger $mint\_gDEF$ will attract more buyers as they will receive more gDEF tokens, and a smaller fee_to_gov will attract more companies to create new ETs as they will receive back a higher percentage from each purchase (if the fees are not redistributed to the governance token holders they will be given to the companies and/or to the developers). This shows the relevant role of governance in balancing between their profitability and the expansion of the protocol to new customers.

Due to the unique architecture of the DEF protocol, it is possible to also define an additional governance level. In fact, each individual company that uses DEF can become similar to a DAO itself and use the created ETs as a governance token for their own company-level governance. This allows them to inquire their users regarding important choices for the company and the holders of the ETs can vote for the proposals or create new ones on their own. These proposals can be about the concerned company operation but also about the use of the DEF protocol itself, as they could suggest to modify the royalty fee or create a new public offering, split the existing ETs and require the payment of dividends.

The protocol therefore changes the way stakeholders interact with the company they are part of, as they can now have a continuous influence on the direction the company is moving towards, and minor investors can also actively participate in choices and changes.

3   Limitations

The biggest risk for users who participate in this protocol comes from companies that could renounce on their projects after attracting buyers for their ETs. This risk is intrinsic to the blockchain space, as it offers a partial anonymity and even if the culprit is found it is

difficult to prosecute legally. To partially mitigate this issue, the protocol offers the collateral mechanism as a way to insure the buyers in case of fraud, reimbursing them a part of their investment. However, the company itself decides whether to provide a collateral, and thus the users have to carefully choose where to invest. An additional solution could be to integrate an optional KYC (Know Your Customer) process before creating the ETs so that the buyers can see which companies have provided the required documents and have some reliable information about them. Ultimately, however, DEF leaves it up to investors to be reasonable in their investments and not to invest in companies which do not appear reliable.

A more technical limitation lies with the bankruptcy and collateral mechanism, which leaves some potential for malicious users to exploit it. Notably, as bankruptcy is declared by majority vote, it would be possible for a malicious user to issue a scam token, and keep just over half of the ETs to prevent the other ET holders from ever passing the bankruptcy vote. To remedy this, methods could be developed to override the majority vote and impose a bankruptcy, for example by using oracles to verify the company's activity on and off the Blockchain. However, malicious users will always find a way to cheat the system; in this case, the only surefire method would be for token holders to call on the DEF governance to impose bankruptcy; this should always be the last-resort method.
Inversely, users could scam an honest company by imposing bankruptcy on them just to get the collateral, for example if their collateral payout is of greater value than the resale of their ETs. Here again, more complex methods could be used to impose that bankruptcy can only be declared once certain quantitative conditions are met, for example a large (>90%) drop in the resale value of the ETs. However, here again there might be potential for malicious activity.

Another technical limitation is that it is not possible to have fractions of tokens. Unlike other cases in the market, it is only possible to buy whole portions of tokens. One way to solve this could be to use third parties to act as intermediaries to split the token, charging a service fee. Moreover, if the majority of the platform's liquidity is concentrated in a few users' portfolio , these users could jeopardise the proper functioning of the platform. For this reason, the risk is reduced as the number of users increases: the crypto-assets are not concentrated in the hands of a few and therefore, the risk decreases as the platform become larger. In larger platforms, indeed, it is just the users themselves who assume the financial and non-financial risks of the platforms they operate on. Their interest lies in keeping the security of the platform high, which would otherwise be devalued.

Another major problem might be the so-called vulnerability risk, which describes the possibility that an attacker could find a way to drain the funds allocated in a smart contract due to errors in the code or by exploiting attack vectors. Cyber-attacks are a major risk for all crypto-currencies; in particular, attackers would be quick to jump on any vulnerabilities in a newly released smart contract. Indeed, the Blockchain world is relatively new, and there are new vulnerabilities which are still being discovered. There exist methods to limit these security risks: most major DeFi companies work with third-party companies to provide additonal security on crypto wallets. However, utlimately this problem is intrinsic to

crypto-currencies, and users must simply have trust in the protocol that there are no major vulnerabilities.

For individual users, security risks can be mitigated by taking out insurance policies on their holdings. As conventional insurance providers are not able to accurately assess the value of crypto assets, there exist specialized DeFi insurance companies such as Nexus Mutual, Eherisc or Cover Protocol. Unlike with traditional insurance, where policies are underwritten by a multinational insurer, premiums on DeFi policies are determined by the community.

4   Conclusion

In this paper we propose a new DeFi protocol which brings the concept of stocks trading to the blockchain. Companies can earn liquidity by putting up equity tokens, which provide buyers with part-ownership of the company and potentially with dividends. Compared to conventional stocks, this system is more democratic: companies do not need to rely on banks for their IPO, and users do not need to rely on banks to buy shares. Consequently, there is a greater variety of shares and of investors.

The biggest intrinsic limitation of the protocol is that, as there are fewer checks to produce an ET, it becomes easy for so-called 'mercenaries' to produce fraudulent tokens which they sell, then collect the profits from and disappear. There are ways to mitigate this risk, notably using mechanisms such as the collateral mechanisms discussed above, or third party services such as KYC to verify company identity. Despite this, the risk remains, and ultimately it is up to the investors to choose reliable companies. Future directions for the protocol will be to find ways to further mitigate the risk, and to defend the protocol against new forms of mercenaries.

In conclusion, the DEF protocol provides an attractive option both for companies and for investors to conventional stocks. DEF cuts out the influence of banks and allows people to trade directly with each other over the primary market. Additionally, DEF makes important strides forward in terms of inclusivity, allowing users from all backgrounds to participate. We believe that the fundamental concept makes sense; for the future of the protocol, there should be constant development to keep DEF relevant and safe from malicious users.

Bibliography

[1] Cristiano Bellavitis Yan Chen. "Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System". In: (2019), pp. 1–27. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418557.

[2] Columbia University. *What is Financial Technology (FinTech)? A Beginner's Guide for 2022*. 2022. URL: https://bootcamp.cvn.columbia.edu/blog/what-is-fintech/.

[3] Peter Roosenboom Thomas Lambert Daniel Liebau. "Security token offerings". In: (2021), pp. 301–320. URL: https://link.springer.com/content/pdf/10.1007/s11187-021-00539-9.pdf.

[4] Morgan Stanley. *7 Insights from Asset Owners on the Rise of Sustainable Investing*. 2020. URL: https://www.morganstanley.com/ideas/sustainability-investing-institutional-asset-owners.

[5] Primavera De Filippi Samer Hassan. "Decentralized Autonomous Organization". In: (2021), pp. 1–10. URL: https://www.econstor.eu/bitstream/10419/235960/1/1764253469.pdf.

[6] *EIP-721: Non-Fungible Token Standard*. 2018. URL: https://eips.ethereum.org/EIPS/eip-721.

[7] *EIP-2981: NFT Royalty Standard*. 2020. URL: https://eips.ethereum.org/EIPS/eip-2981.

[8] *EIP-20: Token Standard*. 2015. URL: https://eips.ethereum.org/EIPS/eip-20.

A   Appendix: Solidity Code

The code below shows an implementation of the DEF protocol in Solidity. Please note that the version of DEF implemented in this code is not exactly the same as what is described in the report above: firstly, it is not complete and secondly, for the report we consider a token following the ERC-721 standard, while the code implements a token following the ERC-20 standard. However, the basic functioning and goals are the same.

```solidity
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.4;
3
4  import "./EquityToken";
5
6  contract DEFplatform {
7
8      address owner = msg.sender; //deployer of contract owns DEF platform
9
10     //fees
11     uint ipoFee = 0;
12     uint facilitationFee = 1; //percentage owner gets whenever a mint of
             an EQT is done
13
14     //registered EQTs
15     uint eqtCount = 0;
16     mapping(uint => EquityToken) public eqts; //companyId => address to
             company's personal EQT contract
17
18     //collateral locked by
19     //to ensure unique symbols for every EQT
20     mapping(string => bool) public symbolTaken;
21
22     //launch company
23     function ipo(
24         string memory _name,
25         string memory _symbol,
26         uint _amountToRelease, //amount of EQT offered to public (caps the
                 total supply of EQT and thus the mintable EQT amount)
27         uint _ownShare, //number defining how much EQT should be minted to
                 owner of company during IPO
28         uint _price
29     ) payable {
30         require(symbolTaken[_symbol] == false);
31         EquityToken eqtContract = new EquityToken(
32             msg.sender,
33             _name,
34             _symbol,
35             _amountToRelease,
36             _ownShare,
37             _price,
38             address(this)
```

```
39          );
40          eqts[eqtCount] = eqtContract;
41          eqtCount++;
42      }
43
44      //functions for owner
45      // Modifier to check that the caller is the owner of
46      // the contract.
47      modifier onlyOwner() {
48          require(msg.sender == owner, "Not owner");
49          _;
50      }
51
52      function setIpoFee(uint _newFee) onlyOwner {
53          ipoFee = _newFee;
54      }
55
56      function setFacilitationFee(uint _newFee) onlyOwner {
57          facilitationFee = _newFee;
58      }
59 }
```

```
 1 // SPDX-License-Identifier: MIT
 2 pragma solidity ^0.8.4;
 3
 4 import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
 5 import "@openzeppelin/contracts/token/ERC20/extensions/draft-ERC20Permit.
     sol";
 6 import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Votes.sol";
 7
 8 import "./DEFplatform";
 9
10 contract EquityToken is ERC20, ERC20Permit, ERC20Votes {
11     DEFplatform immutable defPlatform; //instance of DEF platform to
           enable interaction between EQT contract and platform
12
13     address issuer; //address of entity issuing EQT
14     uint issuedAmount;
15     uint price;
16     uint collateral; //optional collateral tied to EQT to make it less
           risky
17
18     constructor(
19         address _issuer,
20         string memory _name,
21         string memory _symbol,
22         uint _amountToRelease, //amount of EQT offered to public (caps the
               total supply of EQT and thus the mintable EQT amount)
23         uint _ownShare, //number defining how much EQT should be minted to
               owner of company during IPO
24         uint _price,
25         uint _defPlatformAddress
```

```
26      ) ERC20(_name, _symbol) ERC20Permit("EquityToken") {
27          issuer = _issuer;
28          issuedAmount = _amountToRelease;
29          price = _price;
30          defPlatform = DEFplatform(_defPlatformAddress);
31
32          //mint EQT for issuer
33          mint(_issuer, _ownShare);
34      }
35
36      function mint(address _account, uint256 _amount) payable {
37          require(this.totalSupply + _amount <= issuedAmount, "Not enough
                free EQTs mintable");
38          require(price*_amount <= msg.value, "Not enough money to buy EQTs"
                );
39
40          // pay mint and fee
41          uint fee = DEFplatform.getFacilitationFee();
42          (bool paidMint, ) = issuer.call{value: (price-fee)*_amount}("");
43          (bool paidFee, ) = DEFplatform.getOwner().call{value: fee*_amount
                }("");
44
45          //if payments successful, mint tokens
46          require(paidMint && paidFee, "Failed to pay transfer");
47          _mint(account, amount);
48      }
49
50      //functions only issuer of EQT can use
51      modifier onlyIssuer() {
52          require(msg.sender == issuer, "Not issuer of EQT");
53          _;
54      }
55
56      //for e.g. when current issuer sells EQT to another address
57      function setIssuer(address _newIssuer) onlyIssuer payable {
58          issuer = _newIssuer;
59      }
60
61      // The following functions are overrides required by Solidity.
62      function _afterTokenTransfer(address from, address to, uint256 amount)
63          internal
64          override(ERC20, ERC20Votes)
65      {
66          super._afterTokenTransfer(from, to, amount);
67      }
68
69      function _mint(address to, uint256 amount)
70          internal
71          override(ERC20, ERC20Votes)
72      {
73          super._mint(to, amount);
74      }
```

```
75
76     function _burn(address account, uint256 amount)
77         internal
78         override(ERC20, ERC20Votes)
79     {
80         super._burn(account, amount);
81     }
82 }
```