ИКОНОМИЧЕСКИ ИЗСЛЕДВАНИЯ
ECONOMIC STUDIES

Volume 31(4), 2022

Svetoslav Borisov[1]

DEFI – POTENTIAL, ADVANTAGES AND CHALLENGES[2]

Blockchain technology may decrease transaction costs, promote decentralised platforms and build distributed trust, paving the road to new business models. In the financial sector, blockchain technology approves the progress of more innovative, boundless and clear decentralised financial services. Decentralised financial services can broaden financial encompassment by promoting open access and innovation. By scraping out several restrictions, they reveal new opportunities for entrepreneurs and innovators. A year ago, the whole value locked in DeFi (Decentralised finance) systems was almost $600 million, and by May 2021, it was about $88 billion. The frantic development of the ecosystem requires newcomers to understand its basic characteristics. The purpose of this paper is to estimate the advances of decentralised finance, classify current business models, and outline potential challenges and constraints.

Keywords: decentralised finance; blockchain; cryptocurrencies; smart contracts
JEL: O31; D86; L14

1. Introduction

Blockchain technology and distributed ledger (DLT) have obtained immense acceptance since the creation of Bitcoin more than a decade ago (Nakamoto, 2008). The initiation of a distributed, open and distributed ledger allows for censorship-resistant limitless financial transactions between customers. In addition to regular financial transactions, a lot of DLTs maintain scripts for their transactions, supporting customers to set complex payment terms and conditions. Some blockchains, such as Ethereum, even authorise payments to depend on the execution of full Turing programs, so-called smart contracts (Buterin, 2020). 'Decentralised Finance' (DeFi) is neither a legal nor a technical term. In addition to this, DeFi, a new sub-field of blockchain, specialises in improving financial technologies and services on top of smart contract enabled ledgers (Schär, 2020). However, it is progressively employed in the future transformation of finance and its regulation. Typical usage includes one or more components of: (i) decentralization; (ii) distributed ledger technology and blockchain; (iii) smart contracts; (iv) disintermediation; and (v) open banking (Leonhard, 2019). The determination of all DeFi protocols and utilisation is smart contracts, a term that

[1] *Svetoslav Borisov, Chief Assistant Professor, PhD, University of Economics – Varna, phone: 0889440855, e-mail: svetoslav_borisov@ue-varna.bg.*

[2] This paper should be cited as: *Borisov, S. (2022). DeFi – Potential, Advantages and Challenges. – Economic Studies (Ikonomicheski Izsledvania), 31(4), pp. 33-54.*

is commonly assigned to small applications gathered on a blockchain and running on a large network consisting of plenty of computers. Smart contracts to some extent, are ineffectual in comparison to common centralised calculations. On the other hand, their superiority is the high level of security, in the perception that smart contracts ensure deterministic performance and permit everyone to check the resulting changes in status. When accomplished securely, smart contracts are extremely transparent and reduce the risk of manipulation and arbitrary interference. Smart contracts have access to a full set of Turing instructions and are accordingly quite completely. Moreover, they could store cryptocurrencies and thus act as a custodian, with fully adaptive criteria for how, when and to whom these assets can be honoured. This approves a wide variety of interesting applications and thriving ecosystems.

To accept the novelty of smart contracts, we must first look at ordinary server-based web applications. When somebody interacts with such an application, he cannot follow the internal logic of the application. Furthermore, the user does not control the environment of execution. Either one (or both) can be manipulated. As a result, the customer should trust the service provider. One of the blockchain's major innovations is the transfer and trade of financial assets out of credible intermediaries (Wüst, Gervais, 2017). Smart contracts alleviate both issues and guarantee that the application works exactly as anticipated. The contract code is saved in the main blockchain and can therefore be viewed publicly. The behaviour of the contract is determined and the requirements of functions (in the form of transactions) are processed simultaneously by hundreds of participants in the network, ensuring the legitimacy of performance. When execution results in changes in the balance, such as a shift in account balances, these modifications are subject to the consensus rules of the blockchain network and will be reflected and protected by the blockchain status tree.

The initial idea of smart contracts was introduced by Szabo (1994). He uses the vending machine to evolve further the concept and argues that a lot of agreements can be "embedded in the hardware and software we work within such a way as to make a dereliction of contract costly to the infringer". Buterin (2013) proposed a blockchain-based platform for smart contracts to resolve all trust problems concerning the execution environment and provide secure global states. Furthermore, the platform enables contracts to collaborate. The idea was additionally characterised by Wood (2015) and enforced under the name Ethereum. Despite the numerous alternatives, Ethereum is the biggest platform for smart contracts in terms of market capitalisation, convenient applications and advancement activities (Wood, 2014).

Many commonly centralised financial tools are now implemented and utilised in distributed blockchain systems employing smart contracts. This market sector has become known as decentralised finance (DeFi, henceforth) and has gained popularity as projects have emerged to meet the needs of a wide variety of cryptocurrency users and enthusiasts. Decentralised finance is a movement in the space of the blockchain, which has recently attracted increasing interest. The term is usually assigned to open financial infrastructures created on public platforms for smart contracts, such as the Ethereum blockchain (Buterin, Vitalik, 2014).

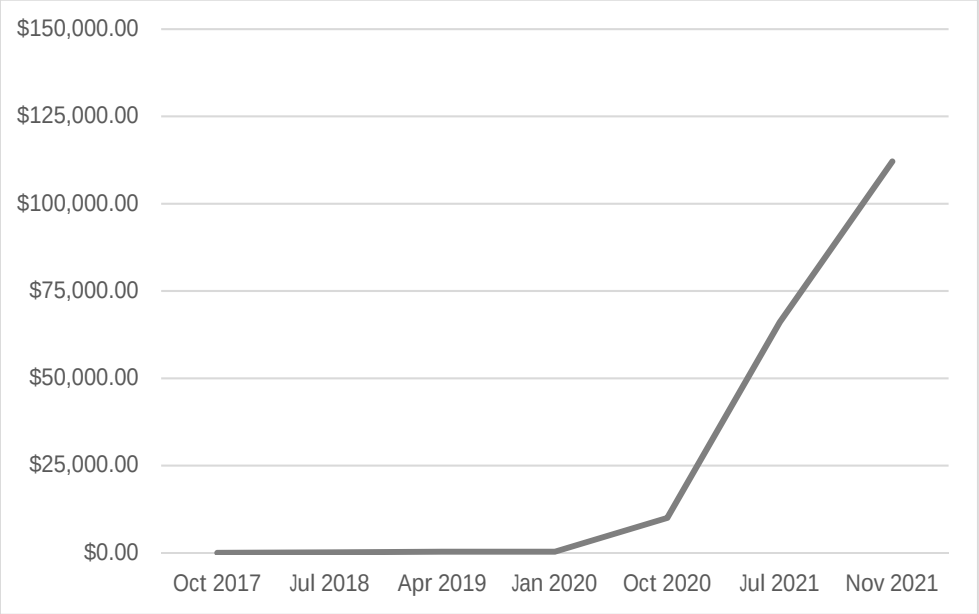
Unlike the conventional financial sector, DeFi does not depend on intermediaries and centralised institutions (Antonopoulos, 2018). Rather, it is established on open protocols and decentralised applications (DApps). The agreements are implemented by smart contracts, transactions accomplished in a safe and deterministic way, and the changes are legitimised on a public blockchain. In such a way, this architecture can create a consistent and supremely

interoperable financial system with exceptional transparency, equivalent access rights and little need for trustees, central clearinghouses or escrow services, as most of these functions can be taken over by smart contracts.

DeFi is still a market alcove with comparatively low volumes, but growing at a rapid pace. The amount of funds locked in DeFi-related transactions has recently reached $88 billion. It is important to understand that these are not values of volume or market capitalisation, but a value related to reserves that are locked in smart contracts for operation in various ways. Figure 1 shows the US dollar asset values locked in DeFi applications.

Figure 1

Total locked value in DeFi contracts (MM USD)



Source: Defipulse.com (2021).

DeFi already proposes a broad array of applications. For example, stable US dollar-backed coins can be purchased on decentralised exchanges (Moin, Sekniqi, Sirer, 2020), it is possible to move these tokens to evenly decentralised lending platforms to receive interest and then add tokenised interest-bearing instruments to a decentralised liquidity pool of blockchain-based investment fund. DeFi's main innovation is similar to a blockchain: reducing the need for trust by substituting centralised platforms with a decentralised system. The emerging system is treated as untrustworthy, which means that no party needs to be trusted to accumulate funds and send transactions. The decentralised character also decreases people's influence on fees and circumstances for employing the system, which is rather transparently governed by supply and demand. Furthermore, DeFi systems are open to everyone. In particular, this means that people can play roles as lenders that have traditionally been in the hands of big players, such as banks.

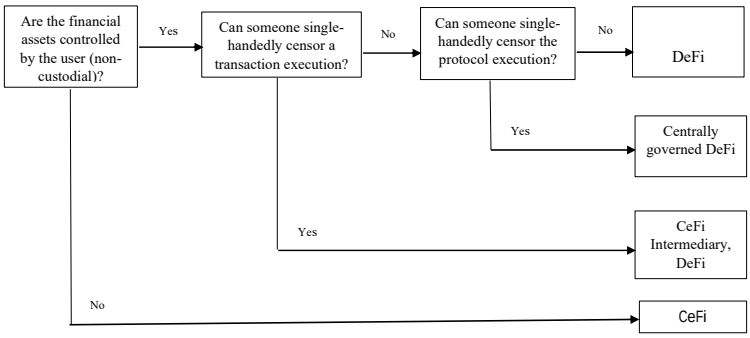
The *subject* of this study is DeFi (decentralised finance), and the *object* is the elucidation of the potential, advantages and challenges for the mass penetration of DeFi. The *purpose* of this paper is to estimate the advances of decentralised finance, classify current business models, and outline potential challenges and constraints. On the ground of a literature review and a comparative analysis between the traditional financial system (CeFi) and DeFi platforms, the following hypothesis is defended: *DeFi platforms solve some problems such as inefficiency, centralised control, limited access, opacity, and lack of interoperability inherent in CeFi.*

2. The Potential of DeFi

Decentralised finance is an entire environment of financial services implemented through smart contracts located in publicly distributed accounting registers. This new proposal intends to decentralise the common financial system by producing services and applications that are detached from reliable intermediaries, allowing unreliable peer-to-peer transactions (Ammous, 2015). Instead of relying on common financial service providers, which are followed by high costs, protracted processes and deficiency of transparency, DeFi implements decentralised financial services. So, applications such as lending, derivatives and trading are automatised and accomplished transparently, reliably and without the requirement for trust (Holotiuk, Pisani, Moormann, 2017). Through the use of publicly accessible protocols, decentralised applications (dApps) and smart contracts, DeFi allow people to play both roles in financial transactions by consuming and providing services, thus "challenging finance, what the Internet did to the media by decomposing the invention of new financial instruments" (Medium.com, 2019).

Figure 2

The boundary between CeFi and DeFi



Source: Qin et al., (2021).

Qin et al. have created a methodology that emphasises borderlines between CeFi and DeFi (Qin et al., 2021). They ask three questions. The first one is whether the financial assets are held by the user, i.e. whether the customer holds control over its assets. If the customer is not in control, i.e. does not hold custody nor can transact the assets without a financial intermediary, that is an example of CeFi. The second one is whether someone can unilaterally

censor a transaction execution. Such a dominant intermediary points to the existence of a CeFi intermediary, as long as the asset settlement can still take place in a decentralised, DeFi-compliant manner. At last, Qin et al. ask the question of whether an entity can single-handedly break, or forbid the protocol's execution. Supposing that this is the case, they should assert that the DeFi protocol is centrally managed. If the answer is negative, then the protocol in question could be qualified as a pure DeFi protocol. Figure 2 illustrates the methodology of Qin et al.

2.1. DeFi vs. CeFi

This chapter provides specific DeFi solutions to the five drawbacks of CeFi: inefficiency, centralised control, limited access, opacity, and lack of interoperability inherent in traditional financial systems.

2.1.1. Inefficiency

DeFi may realise financial transactions with high volumes of assets and low friction, which is generally an enormous administrative burden for CeFi. DeFi builds reusable smart contracts in the shape of dApps projected to execute a particular financial operation. These dApps are accessible to any customer who looks for a specific kind of service, no matter what the size of the transaction is, for instance, a put option execution. To a great extent, a customer may self-serve inside the range of existing smart contracts and blockchain within the application. In the case of Ethereum-established DeFi, the contracts may be utilised by anybody who pays the flat gas fee, commonly around $0.15 for a transfer and $2.00 for a dApp characteristic such as leveraging opposite to collateral. Once redistributed, these contracts constantly support their service with near-zero administrative overhead.

One of the formations in DeFi that advances efficiency is Keepers. They are extrinsic members directly motivated to supply a service to DeFi protocols, such as auditing positions to safeguard that they are fully collateralised or triggering state updates for differing functions. To assure that a dApps' advantages and services are optimally priced, keepers' rewards are frequently structured as an auction. Pure, clear competition adds value to DeFi platforms by assuring customers pay the market price for the services they demand.

A different conception that likewise encourages efficiency is a fork. A fork, in the framework of open-source code, is a copy and reuse of the code with upgrades or improvements layered on top. A typical fork of blockchain protocols is to link them into two parallel currencies and chains. Doing so builds competition at the protocol level and constructs the best conceivable smart contract platform. Not only the code of the whole Ethereum blockchain is public and forkable, but each DeFi dApp developed on top of Ethereum as well. If inefficient or suboptimal DeFi applications occur, the code may be effortlessly copied, advanced, and redeployed through forking. Forking and its advantages rise from the open character of DeFi and blockchains.

2.1.2. Centralised Control

The second drawback of CeFi is the powerful control exercised by governments and big institutions, allowing for a monopoly over parameters such as the money supply, rate of inflation, and admission to the best investment opportunities. In contrast, the society of stakeholders or even a prearranged algorithm may control an element, such as the inflation rate, of a DeFi dApp. If a dApp includes distinctive rights for an administrator, all customers are knowledgeable of the rights, and any customer may effortlessly discover a less-centralised counterpart. DeFi reverses this centralised control by transferring control to open protocols with transparent and unchangeable settings (Schilling, Uhlig, 2019). As no central authority governs or coordinates access to the decentralised environment, customers control their data and store their financial resources themselves. Because customers can save their entry tokens, i.e., signing keys and allowing their transactions, they are completely self-contained. While this, on the one hand, prevents theft or confiscation of funds by a centralised party, individual users, on the other hand, are not protected against the loss of their access tokens, as only they can recover them.

While distributed ledgers do not depend on a specific operator as a trusted agent, they instead distribute trust in a network of nodes (Anjum, Sporny, Sill, 2017). System security is based on the assumption that sufficient nodes in the network are kept fair so that they can reach a consensus on the validity of transactions (Chen, Bellavitis, no date). Consensus ensures that the system is fixed (meaning that transactions cannot be modified, added or deleted retroactively) and resistant to censorship (sometimes called vitality), which ensures that new valid transactions will eventually be included.

Public blockchains are composed to be open, which means that they do not set entry rules and everyone can collaborate with them. DeFi applications assembled on public blockchains derive these attributes by default. Approvals can exclusively be included if DeFi platforms are established on a private blockchain with supplementary entry restrictions or by determining further permissions in the code (Grech, Camilleri, 2017). This also allows anybody to participate in speculation or margin trading, which is not accessible to anybody when utilising centralised platforms, as specific restrictions request (Xu et al., 2017).

The open-source origin of blockchain and the public character of all smart contracts ensures that drawbacks and inefficiencies in a DeFi project may be easily recognised and "forked away" by customers who copy and advance the impaired project. Therefore, DeFi endeavours to invent protocols that instinctively and delicately motivate stakeholders and keep up a robust equilibrium through cautious mechanism design. Naturally, trade-offs exist between having a centralised party and not having one. Centralised control permits for radically definite action in a crisis, sometimes the imminent approach but likewise perhaps an overreaction. The course to decentralising finance will assuredly confront increasing problems because of the challenges in pre-planning for every eventuality and economic nuance. Conclusively, nonetheless, the transparency and security acquired through a decentralised approach will conduce to powerful, robust protocols that may turn into trusted financial infrastructure for a universal customer base.

2.1.3. Limited Access

As smart contract platforms lead to more-scalable applications, customer friction descends, allowing a broad range of customers and thus diminishing the third drawback of CeFi: limited access. Not limited to the DeFi space, but widespread in it, is the aspect of transforming smart contracts within decentralised autonomous organisations (DAO). By allowing the community to propose legislation and vote based on their share of the proposal, management is distributed. The three central aspects of management – joint incentives, accountability and transparency are realised through the creation of consumers and investors accountable for the success of the ecosystem.

It is rare for CeFi markets to operate without downtime. For example, the New York Stock Exchange and the Nasdaq Stock Exchange are the two major trading venues in the United States, and their business hours are Monday to Friday from 9:30 a.m. to 4 p.m. Eastern Time. Due to the non-stop nature of blockchains, most if not all DeFi markets are open 24/7. As a result, DeFi does not have pre-or post-market trading compared to CeFi whereby liquidity on a range of products is typically thin during these periods. Furthermore, system outages at CeFi stock exchanges and CeFi cryptocurrency exchanges have been known to occur due to numbers of users attempting to access the exchanges during times of volatility, such as the GameStop short squeeze event, not to mention the intervention by brokerage firms to restrict their respective customer's purchase and sale of certain equity products due to liquidity and solvency concerns (Robinhood.com, 2021).

DeFi contributes broad underserved groups, such as the worldwide community of the unbanked also small businesses that use large shares of the labour force (for instance, almost 50% in the United States) direct access to financial services. The subsequent effect on the whole global economy shall be strongly positive. Even users who have admission to financial services in CeFi, such as bank accounts, mortgages, and credit cards, do not have admission to the financial services with the best competitive pricing and best agreeable terms; these services and structures are limited to big institutions. DeFi permits any customer access to the wholeness of its financial infrastructure, despite his wealth or geographical region.

A case of resolving the limited access issue is yield farming. This practice affords access to many who demand financial services but whom CeFi drops behind. To sum up, yield farming produces inflationary or contract-funded prizes to customers for staking capital or using a protocol. These prizes are payable in the identical basic asset the customer owns or in a different asset such as a governance token. Any customer can engage in yield farming. A customer may stake an amount of any size, despite how modest, and receive a proportional prize. This ability is specifically strong in the example of governance tokens. A customer of a protocol that distributes a governance token via yield farming turns into a partial owner of the platform through the issued token. A rare situation in CeFi, this mechanism is an ordinary and celebrated manner to provide ownership of the platform to the people who utilise and benefit from it.

2.1.4. Opacity

The fourth flaw of CeFi is opacity. Most publicly distributed accounting records provide transparency by default, as all transactions saved in the blockchain are publicly seeable. Transaction senders and recipients are identified by aliases, while transaction values and submitted data are sent clearly and specifically. Unless additional confidentiality measures are taken, it has been demonstrated that transactions can be related and customers can be recognised (Meiklejohn et al., 2013). For DeFi applications, basic transparency means that all use and stored funds are public at all times. DeFi delicately resolves the problem of opacity through the open and contractual character of agreements. It is worth investigating how smart contracts and tokenisation promote transparency inside of DeFi.

Smart contracts bring an instantaneous advantage in terms of transparency. All parties are enlightened of the capitalisation of their counterparties and, to the degree necessary, may see how funds will be redistributed. The parties may observe the contracts themselves to determine if the terms are acceptable and to remove any uncertainty that may occur when they collaborate under the contract terms. This transparency alleviates the risk of legal burdens to a large extent and brings peace of mind to minor players. In the current environment of CeFi, they could be exploited by dominant counterparties through postponement or even completely inhibiting their end of a financial agreement. In practice, the average user does not comprehend the contract code, rather, he or she depends on the open-source character of the platform and the knowledge of the crowd to sense security. In general, DeFi diminishes counterparty risk and hence establishes a host of efficiencies not demonstrated under CeFi.

DeFi participants are responsible for performing under the terms of the contracts they utilise. One procedure for guaranteeing the proper behaviour is staking. Staking is escrowing a crypto-asset into a contract so that the contract discharges the crypto-asset to the suitable counterpart only after the contract terms are met; alternatively, the asset returns to the initial owner. Counterparties may be requested to stake on any claims or cooperations they execute. Staking carries out agreements by charging a tangible penalty for the offending side and a tangible prize for the cooperation. The tangible prize shall be at least as good as the result of the initial terms of the contract. These transparent incentive systems produce more reliable and clearer assurances than CeFi agreements.

2.1.5. Lack of Interoperability

The fifth flaw of CeFi is the lack of interoperability. CeFi services are complicated to combine, usually requiring a wire transfer, and in many instances cannot be reintegrated. The capabilities for DeFi are considerable and innovations continue to expand at a non-linear rate. This expansion is sustained by the facility of composability of DeFi services. Some blockchain ecosystems, such as Ethereum, maintain vigorous programming instruments that are used for DeFi services. Sophisticated applications, containing auctions, voting and trading can be created with smart contracts. Their functions can be called by customers and smart contracts, which allows for easy connection, arrangement or mixture of extant applications without supplementary programming exertion.

Once a fundamental framework has been established, it is possible to be created synthetic assets and implement new protocols allowing for borrowing and lending. A higher layer would permit for the accomplishment of leverage on top of borrowed assets. Such compatibility may continue in a growing number of directions as new platforms occur. Bringing together contracts to build new kinds of services is often seen as a "Lego" feature of DeFi protocols. This feature stems from the run of smart contracts as creating blocks and linking them to build more useful structures. The benefits of composability, particularly tokenisation and networked liquidity are explained below.

Tokenisation is a critical form in which DeFi platforms coordinate with each other. A good example is a percentage holding stake in a private commercial real estate venture. It would be a challenge for CeFi to collateralise this asset either for a loan or a derivative position backing. As DeFi depends on joint interfaces, applications may straightly plug into each other's assets, repackage, and subdivide positions as required. DeFi can unlock liquidity in traditionally illiquid assets through tokenisation. A typical example would be the creation of fractional shares from an indivisible asset such as a stock. We may expand this conception to provide fractional ownership to scarce resources such as unique art. The tokens may be utilised as collateral for any other DeFi service, such as leverage or derivatives. We are capable to invert this archetype to build token bundles of groups of real-world or digital assets and trade them similar to an ETF. Let's imagine a dApp comparable to a real estate investment trust (REIT), but with the extra proficiency of permitting the owner to divide the REIT into separate real estate components to choose a favoured geographical location and distribution within the REIT. Ownership of the token gives direct ownership of the allocation of the properties. The owner may trade the token on a decentralised exchange to close the position.

Tokenising hard assets, such as real estate or precious metals, is more difficult than tokenising digital assets because the practicable considerations associated with the hard assets, such as maintenance and storage, cannot be executed by code. Legal constraints according to jurisdictions are likewise a challenge for tokenisation; however, the adequacy of secure, contractual tokenisation for nearly all use cases ought not to be undervalued.

The conception of interoperability broadens effortlessly to liquidity in the exchange use case. CeFi exchanges, particularly those that individual investors ordinarily utilise, cannot easily share liquidity with other exchanges without specialised access to a prime broker, which is usually restricted to hedge funds. In DeFi, as a subcomponent of the contract, any exchange application may use the liquidity and rates of any other exchange on the same blockchain. This feature allows for networked liquidity and brings about very competing rates for customers within the same application.

2.2. Overview of the services provided through DeFi

This subsection illustrates the capability of DeFi applications by displaying typical applications. Conditionally, this application can be summarised in the following five sections: lending platforms, asset platforms, decentralised exchanges (DEX), derivative

services and payment networks. While more sections are emerging, the focus of this study will be on these five sections.

- **Lending platforms:**

Decentralised lending services are the biggest class of DeFi outputs, with $28.48 billion in locked funds (Defipulse.com, (2021). They offer loans to companies or individuals utilising smart contracts as intermediaries and mediators. In this way, the "common" intermediaries obligated for centralised lending are eliminated. In connection with the analysis in the previous paragraph, Table 1 illustrates a comparison between CeFi and DeFi lending platforms. These smart contracts automatise the lending agreement, including interest rate rules. Pooled loans utilise float interest rates that object to supply and demand. The funds of all borrowers are gathered in a single, smart contract-based lending pool, and lenders begin to gain interest just when they deposit their money in the pool. Nevertheless, the interest rates are a function of the pool's utilisation rate. When liquidity is easily accessible, loans will be inexpensive. However, during times of high demand, loans will become dearer. Lending pools have the supplementary benefits that they may accomplish maturity and size conversion while maintaining comparably high liquidity for the individual lender.

Table 1

Comparison between CeFi and DeFi – Lending platforms

	CeFi	DeFi
Inefficiency	- Acquiring a loan includes expenses of time and money. - Non-optimal rates for borrowing and lending because of inflated costs.	- Instant liquidity at the press of a button with minimal transaction costs. - Algorithmically pooled and optimised interest rates.
Centralised Control	- Interest rates are affected by the US Federal Reserve and admission to loan services controlled by regulation and institutional policies. - Borrowing and lending rates are controlled by institutions.	- MakerDAO platform is publicly controlled by the MKR holders. - Compound rates are settled algorithmically and provide control of market parameters to COMP stakeholders motivated to transfer value to users. - Aave interest rates are controlled algorithmically.
Limited Access	- Acquiring loans is arduous for a vast majority of the population. - Complication in infiltrating high-yield USD investment opportunities or competitive borrowing. - Exclusively selected groups have access to substantial quantities of money for arbitrage or refinancing.	- Open capability to draw DAI liquidity against an overcollateralised position in any supported ERC-20 token. Admission to a competitive USD-denominated return in the DSR. - Open capability to borrow or lend any supported assets at competing for algorithmically established rates (provisionally subsidised by COMP distribution). - Flash loans democratise admission to liquidity for instantly profitable businesses.
Opacity	- Ambiguous collateralisation of lending organisations.	- Clear collateralisation ratios of vaults discernible to the whole ecosystem.
Lack of Interoperability	- Cannot trustlessly utilise USD or USD-collateralized token in smart contract agreements. - Cannot reuse supplied positions for other investment opportunities. - Cannot monetise or use surplus collateral in a lending position.	- Issuance of DAI, a permissionless USD- tracking stablecoin supported by cryptocurrency. DAI may be utilised in any smart contract or DeFi application. - Tokenised positions through cTokens may be utilised to turn static assets into yield-generating assets. - Credit delegacy enables parties to utilise deposited collateral when they do not require borrowing liquidity.

- **Asset platforms:**

Traditional assets serve mainly as capital collateral for companies. Similarly, virtual assets in the crypto area have comparable goals. Nonetheless, since they are built, saved and traded through the blockchain, they are innately public and their shifts are transparent. Using smart contracts, they may be traded automatically and without restrictions. Assets are the second most valuable class in Defi. Popular assets platforms in the DeFi space are USDT, USDC and BUSD with a locked value in US dollars ($30.97B), ($24.75B) and ($10.68B), respectively (Defipulse.com, 2021).

- **Decentralised exchanges (DEX):**

Services that concentrate on decentralised cryptocurrency and token exchange are frequently classified as DEX and represent the third biggest category of DeFi products, with about $18.92 billion in locked funds (Defipulse.com, 2021). DEX operates likewise to a stock exchange, but rather than being managed by a central provider, the exchange is managed by a smart contract located on a blockchain such as Ethereum. The absence of a centralised authority indicates that the principles and supervisions for trading are prearranged in the code of the smart contract and consumers must interact with it to trade assets. Typically, a smart contract further processes consumer funds during the trading process to assure a proper payout. Concerning the analysis in the previous paragraph, Table 2 presents a comparison between CeFi and DeFi exchanges.

Table 2

Comparison between CeFi and DeFi – Exchanges

	CeFi	DeFi
Inefficiency	- Trades usually demand two parties to settle.	- An AMM (automated market makers) that enables steady access for trading against the contract.
Centralised Control	- Exchanges that control which trading pairs are supported.	- Enables anybody to construct a new trading pair if it does not already exist and automatically transmit trades through the most effective pathway if no direct pair exists.
Limited Access	- The most excellent investment opportunities and returns from liquidity providing are limited to big institutions.	- Anybody may become a liquidity provider and gain fees for doing so. Any project may issue its token on Uniswap to give anybody access to it.
Opacity	- Unidentified if the exchange controls all users' entire balance.	- Transparent liquidity levels in the platform and algorithmic pricing.
Lack of Interoperability	- Capability to trade assets on one exchange is not readily executed within the different financial applications.	- Any token swap required for a DeFi application may use Uniswap as an installed feature.

To discover the swap rate, smart contract-based liquidity pools utilise a variety of fixed product models, where the relative price is a function of the smart contract's token reserve ratio. In its rudimentary form, the fixed product model may be represented as $xy = k$, where x and y coincide with the smart contract's token reserves and k is a constant. Bearing in mind that this equation should uphold when anyone performs a trade, we obtain $(x + \Delta x).(y + \Delta y) = k$. It may then be simply displayed that $\Delta y = (k/(x + \Delta x)) – y$. Therefore, Δy will accept negative values for any $\Delta x > 0$ (Schär, 2020). Any swap is located on a convex token reserve curve. A liquidity pool utilising this model cannot be drained, as tokens will become pricier with lower reserves. When the token supply of either one of two tokens comes nearer zero,

its relative price increases infinitely as an outcome. It is necessary to mention that smart contract-based liquidity pools are not dependent on extrinsic price feeds (so-called oracles). Whenever the market price of an asset changes, anybody may take benefit of the arbitrage opportunity and exchange tokens with the smart contract while the liquidity pool price converges to the present market price.

A different method is to attract liquidity reserves through a smart contract that enables big liquidity providers to link and promote prices for particular trade pairs. A customer who chooses to swap token x for token y can send a trade request to the smart contract. The smart contract will collate prices from all liquidity providers, adopt the best proposal on behalf of the customer, and perform the trade. It operates as an entrance between customers and liquidity providers, guaranteeing the best fulfilment and atomic settlement. In opposition to smart contract-based liquidity pools, with smart contract-based reserve gathering, prices are not set inside of the smart contract. Rather than, prices are determined by the liquidity providers. This method functions excellent if there is a comparably large base of liquidity providers. Nevertheless, if there is restricted or no competition for a certain trade pair, the method can lead to collusion risks or even monopolise price setting. Such corrective, reserve aggregation protocols commonly have some (centralised) control means, such as maximum prices or a minimum number of liquidity providers.

A substitute to classic exchange or liquidity pool models is peer-to-peer (P2P) protocols, ditto called over-the-counter (OTC) protocols. They mainly depend on a two-step method, where participators may request the network for counterparts who would like to trade a given pair of crypto-assets and then bargain the exchange rate bilaterally. Once the two parties agree upon a price, the trade is performed on-chain through a smart contract. Unlike other protocols, suggestions may be approved completely by the parties who have been included in the bargaining. Particularly it is not attainable for a third party to front-run somebody accepting a suggestion by examining the pool of unconfirmed transactions (mempool). For efficient performance, the procedure is mainly automated. Also, one may utilise off-chain indexers for peer finding out. These indexers presume the task of a directory in which individuals may announce their intention to make a particular trade.

Curve Finance (Curve. fi, 2021), whose users have locked in more than $8.16 billion, is the largest example in this category, aiming attention primarily on trading and lending to stablecoins. Another famous DEX service is Uniswap, with over $5.47 billion in the capital (Uniswap.org, 2021). The Uniswap smart contract is publicly applicable on the blockchain, and any customer can interact directly with it. The major mechanic behind Uniswap is the pooling of liquidity, which eliminates the need to process order logs. Consumers pay 0.3% transaction fees, which are added to the liquidity pool used and raise income for liquidity providers.

- **Derivative services:**

Decentralised derivatives are tokens that obtain their value from a basic asset's performance, the result of an event, or the establishment of any other noticeable variable. They commonly need an oracle to trace these variables and consequently present some dependencies and centralised elements. The dependencies may be lessened when the derivative contract utilises numerous independent data sources. Table 3 illustrates a comparison between CeFi and DeFi

derivatives. Tokenised derivatives may be designed without the presence of third parties and in a form that forbids malicious impact. Famous instances of DeFi derivatives are Synthetix ($796.1M) (Synthetix.io, 2021), Nexus Mutual ($359M) (Nexusmutual.io, 2021) and BarnBridge ($294.5M) (Barnbridge.com, 2021).

Table 3

Comparison between CeFi and DeFi – Derivatives

	CeFi	DeFi
Inefficiency	- Fixed income rates are lesser because of layers of fat in CeFi. - Suboptimal rates for borrowing and lending because of excessive costs. - Sizable asset buys suffer from slippage as traders consume into the liquidity pool.	- Lean infrastructure operating on Ethereum permits more vying rates and diversified liquidity pools. - Algorithmically pooled and optimised interest rates. Complimentary flash loans (no collateral) provided for instant use cases. - Synths exchange rates are supported by a price feed, which removes slippage.
Centralised Control	- Fixed income instruments are mainly limited to governments and big companies. - Borrowing and lending rates are controlled by organisations. - Assets may principally only be bought and sold on registered exchanges.	- Yield protocol is open to participants of any size. - dYdX rates are defined algorithmically. - Provide synthetic assets in one spot that may trace any real-world asset.
Limited Access	- Numerous investors have restricted entry to buy or sell complex fixed-income investments. - Hardship in acquiring high yield USD investment opportunities or competitive borrowing as well as futures and derivative products. Admission to capital for instantly gainful initiatives is restricted. - Admission to particular assets is geographically restricted.	- Yield enables any market participator to buy or sell a fixed income asset that settles in a target asset of their preferring. - Open capability to borrow or lend any provided assets at competitive algorithmically defined rates. Involves a continuous futures contract that could synthetically support any asset. Complimentary flash loans produce anybody admission to large amounts of capital to capitalise on arbitrage or different profitable opportunities. - Anybody may access Synthetix to buy and sell Synths.
Opacity	- Risk and unpredictability of counterparty in traditional agreements. - Vague collateralisation of lending institutions.	- Comprehensible collateralisation publicly known on Ethereum blockchain supporting the investment. - Obvious collateralisation ratios of borrowers are visible to the entire ecosystem.
Lack of Interoperability	- Fixed income instruments usually settle in cash which the investor ought to decide how to distribute. - Hard to repurpose funds inside of a financial instrument. - Real-world assets such as stocks can't be readily presented directly on a blockchain.	- yTokens may settle in any Ethereum target asset and even settle synthetically into a floating-rate lending protocol to reserve returns. - Flash loans may instantly use the wholeness of the assets under management for external opportunities without risk or loss to investors. - Synth representations of real assets are completely consistent with Ethereum and other DeFi protocols.

- **Payment networks:**

Even elementary financial instruments such as payments are decentralised to decrease the impact of central payment providers to create an open financial environment. As a result of the essence of blockchain technology, customers can exchange cryptocurrency safely and straight without the commitment of intermediaries. Nonetheless, huge fees and unavoidable

lags require specific services that improve decentralised payments. The core technology for services like Flexa ($1.35B) depends on payment channel technology (Flexa.network, 2021), xDAi ($74.2M) builds side chains (Xdaichain.com, 2021). The above categories are not absolute and represent guidelines for classification, as plenty of features of DeFi are still issue to adjust. In addition, many DeFi services can be identified with more than one or even supplementary groups. Gnosis, for example, can be classified as DEX (decentralised exchange) due to its protocol and as an asset over conditional tokens (event-based assets).

3. Risks and challenges before the implementation of DeFi

3.1. Security

This study determines three features of DeFi products that necessitate distinguished consideration in terms of security: the vulnerability of smart contracts, infrastructure risk and weaknesses in interdependence. The past has proved that insufficient security has led to huge financial losses, with some of the most notorious incidents being cited for clarity.

DeFi products are based on smart contracts that operate directly or indirectly with consumer funds. When more funds are associated with a particular smart contract, it turns more appealing to potential attackers. In this way, smart contracts can be seen as similar to public error programs, as any user who finds an error in the contract may employ the vulnerability and conceivably steal money. The case that the contract code and all past collaborations with it are stored transparently in the blockchain makes it even simpler to detect errors. Accordingly, smart contract developers have to put a lot of work into programming contracts without susceptibilities. Utilising familiar layout templates and best procedures is a good starting point. Further external security audits can also increase confidence in the correctness of the contract. Developers may still construct a contract so that possible security adjustments are enforceable while the contract is running on the blockchain. Nevertheless, such an updated device claims some form of management that efficiently reduces the degree of decentralisation. The past has shown a huge impact of programming errors in smart contracts, for example, on DAO and its respective portfolios (Cryptoslate.com, 2020; Coingeek.com, 2020; Theblockcrypto.com, 2020).

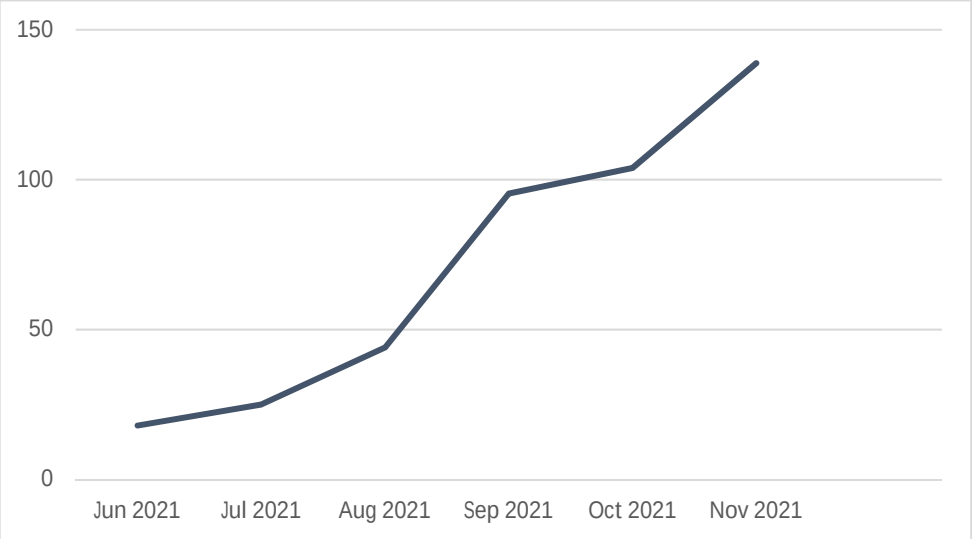
Although the deterministic and decentralised enforcement of smart contracts has its benefits, there is a risk that something will be confused. If there are coding errors, these errors can potentially create vulnerabilities that could enable an attacker to drain a smart contract, induce chaos, or do the protocol unusable. Consumers should be attentive that the protocol is as safe as the smart contracts that underlie it. Unfortunately, the average consumer will not be capable to read the contract code, even less of assessing its security. Although audits, insurance services and official inspections are partial solutions to this problem, some ambiguity remains. Analogous risks remain in the performance of the contract. Most users do not understand the payload of the data they are requested to sign as part of the transactions and can be misguided by a compromised interface.

Next, the core infrastructure may have additional impacts on the DeFi product, which must be taken into account when designing application – distinguishing security means. For

example, the limited bandwidth of the Ethereum blockchain led to network congestion in 2020 (Figure 3). The contract uses expectations to assure timely interplay between the members. In this case, a crowded network can lead to missed user queues, as valid transactions by honest customers may not be recorded on time (Winzer, Herd, Faust, 2019). Therefore, the properties of the basic consensus mechanism affect the application-specific protection properties.

Figure 3

Average weekly price for gas in the Ethereum blockchain denominated in Gwei



Source: Duneanalytics.com, (2021).

Designing new protocols for the DeFi area demands distinctive attention. In particular, due to the ability to constitute distinct DeFi products and build new protocols based on existent ones. The protection of a given protocol cannot be analysed in a stand-alone model: the influences of other protocols ought to also be taken into account. This aspect is emphasised by the presentation of two specific attacks. The first is frontrunning, so-called by Daian et al. (Daian et al., 2020). The term ex-ante control covers all scenarios in which one party attempts to record its transaction before the competing transaction. Any attempt at initial implementation could lead to a so-called "priority gas auction", in which customers substitute as the price of gas increases for their transactions. The idea is for the miners to be stimulated by including their transactions in the block as a priority.

Finally, due to the great interest in DeFi, the system is becoming increasingly attractive for attacks and fraud. In September 2020, it was revealed that several tokens had been used in a "pump and dump" scheme (News.bitcoin.com, 2020). Influencers disseminated information about this token to encourage other users to invest in it. Once the price of the token was high enough, the major investors sold their shares to get a great return on investment.

3.2. Limited scalability

Blockchain technology and its functions deteriorate from restricted transaction throughput, which is frequently seen as a major obstacle to the widespread adoption of this technology (Abra.com, 2019). The main reason is that the blocks in the registry have only a restricted space shared by transactions, implementation of smart contracts and requirements of the contract functions. Therefore, when plenty of applications and their customers contend for restricted block space, miners choose the transactions that suggest the largest fees. Thus, consumers have to adopt either very large fees or lengthy delays to confirm new transactions.

Ethereum is the main choice for DeFi applications due to its programmability, wide community and wide array of developer instruments. Nevertheless, due to its restricted scalability, Ethereum cannot cope with the increasing number of customers and arising DeFi applications. An analysis by the German digital business association Bitkom says it is extremely controversial whether Ethereum is a viable platform for DeFi, exceptionally when even more customers log into the system (Bitkom.org, 2020). When demand for DeFi applications raised in the late summer of 2020, Ethereum's transaction fees raised dramatically and built plenty of other applications on the blockchain platform impossible.

3.3. Oracles

While the collaboration among two chains, such as smart contracts, is easy, the transmission of data from extrinsic sources and websites to a smart contract builds new challenges. Plenty DeFi products depend on extrinsic information such as exchange rates provided by so-called oracles. As the data obtained from these oracles influence the behaviour of smart contracts and consumers, the challenges posed by the transfer of external data along the chain are considerable anxiety. More precisely, the security of these DeFi products is established on the dependability, accuracy and correctitude of the information provided by the oracles. Oracles introduce dependencies and, in some cases, can lead to a highly centralised performance of the contract. To diminish this risk, plenty of projects depend on large oracle networks with M-of-N data schemes. Oracles are therefore evaluated based on their accountability for transparency and the required level of confidence. Popular products based on DeFi oracles are Maker (Makerdao.com, 2021), Compound (Compound.finance, 2021), AmpleForth (Ampleforth.org, 2021) and Synthetix (Synthetix.io, 2021). ChainLink even offers a network of oracles that do information approachable through its API (Chain.link, 2021). Its growing importance is likely to be associated with important partnerships, such as Google, Oracle or Salesforce.

The Maker project mitigates some of the defiances listed above by linking data from numerous sources rather than depending on data from an individual source. For each kind of extrinsic data, a set of oracle whitelists is defined, which often supply examples. These examples are combined by an aggregator that generates the concluding data addressed to the platform. Therefore, the dependability of oracle data is enhanced through copy. The oracles used must be independent so that the failure of one oracle does not affect other oracles. The aggregator calculates the median of the reported samples to cancel any large deviation. In addition, Maker provides the ability to update the white list of oracles, which leads to the

swap of oracles. The update is established on the verdict of the managers governing the MKR token.

Liu et al., after examining the DeFi oracles, introduce large-scale calculations of price volatility, downfalls, and transaction activity examinations (Liu et al., 2020). In addition, the authors offer recommendations for designing oracle decisions. First, each oracle must indicate information such as data sources, frequency of updates, and description of price variations. Such common information may be easily supplied and significantly increases transparency by allowing consumers to comprehend where the fluctuations from distinct sources come from. Second, because oracles do as credible third parties, it ought to be possible to hold them accountable for misconduct such as missing reports or large price deviations. This can be achieved by including inducements in the scheme of Oracle solutions. For instance, oracle operators win rewards when the frequency and accuracy of their emissions are adequate. On the other hand, the penalty for poor performance can be realised by denying awards and probably even withdrawing crypto assets from a previously provided pool.

3.4. Regulations

The creation of unified global standards to regulate the crypto-economy may alleviate risks such as censorship or collusion, but to date, they do not exist. As the DeFi market raises in size and effect, it will require large regulatory inspections. Most existing regulatory concepts still deal mainly with the classification of tokens for tax purposes. The Liechtenstein and US governments operate as worldwide role models, and regulators, in general, have increased clarity by following suit (Consensys.net, 2019). For DeFi, it is not yet clear how the generated income is regulated. The correct status of the whole environment as such is not undoubtedly determined. Questions arise about the possibility of abuse or illegal use. However, it is often unclear whether the ecosystem may even face a shutdown. An example in this context is an algorithmic stablecoin venture identified as Basis. It was forced to cease its activities due to regulatory concerns in December, 2018. The worrying message on their homepage serves as a warning to similar future undertakings: “Unfortunately, having to apply US securities regulation to the system had a serious negative impact on our ability to launch Basis. As such, I am sad to share the news that we have decided to return capital to our investors. This also means, unfortunately, that the Basis project will be shutting down” (Basis.io, 2018).

Punishing a particular use is difficult due to the aspects of self-reading and decentralised completion of transactions. There is a critical chasm between management and external regulation that needs to be filled regarding Ethereum’s DeFi. In addition, the lack of information about your customer (KYC) processes in the DeFi environment makes it difficult for regulators to admit it as an official financial field. KYC practices are difficult to apply. As a result, regulators face the great challenge of not inhibiting innovation too much when regulating DeFi. Yeung (2009) asserts that the equilibrium between legal and technical code maintains interplays with distinct aspects (economic, political, social) without hurting the society (Yeung, 2019).

In September 2020, the European Commission has introduced a project to regulate "crypto-assets" (digital, blockchain-based assets), which is anticipated to enter into force by 2023. The Regulation "Crypto Asset Markets" (MiCA), which is straightforwardly suitable to all European countries. Member States define the broadest regulation of digital assets to date. As far as DeFi is concerned, it is not yet clear what the consequences of this project are. Although the project contains most kinds of crypto assets and classifies them variously, DeFi tokens are not expressly addressed. The DAI stablecoin may be categorised as a so-called asset-referenced Token according to the project (European Commission, 2020). The classification is justified by the soft attachment to the lucky dollar. Yet many tokens and contracts may be reflected as "issuer-free". This is a key issue in this context. Probably smart contracts in the DeFi area can be categorised at some point as crypto asset service producers. However, convincing legal research needs to be done to further explain the connection with DeFi.

A great number of large market-cap cryptocurrencies have been decreed as commodities by the CFTC, which exempts them from monetary circulation laws. Some states, though, such as New York, have a regulation that targets brokerages with a focus on the transfer and swap of cryptocurrencies. As DeFi keeps on to spread and the total number of released assets continues to rise, it is anticipated to foresee enhancing special and nuanced regulations directed at DeFi protocols and their customers. Cryptocurrency taxation has yet to be completely established from a regulatory point of view, and accounting software/on-chain supervising is just starting to approach mainstream retail audiences. As long as the DeFi are subjected to new regulations (virtually daily), such as permitting banks to be cryptocurrency custodians, the market outlook for these institutions is murky.

3.5. On- and Offramping

Usefulness and user experience can ascertain the destiny of projects. Since DeFi was originally designed by experienced crypto users, they were created primarily for their needs. So far, the design of several decentralised applications (dApps) has been essentially ameliorated. Nevertheless, the terms of application are often clarified at a high technical level or are completely ingrained in financial jargon. In the long run, this poses a threat to the mass acceptance of some DeFi projects. An attainable resolution may be to guide inexperienced customers through the workflow in a tutorial way, showing consequences in progress (whilst providing a link to a clarification).

On- and off-ramping attribute to the approaches of swapping conventional assets for crypto-assets and vice versa. Centralised exchanges are established on confidence in an intermediary, request authentication through KYC practices, have restricted scalability, suffer from security problems, process off-chain transactions and impose significant fees (Medium.com, 2018). Many of these shortcomings are equivalent to the constraints faced by traditional banks. The superior centralised exchanges are Coinbase, Binance and Kraken. To ensure seamless on- and off-ramping, these companies need to grow significantly to meet the requirements of all customers.

3.6. Confidentiality

The fact that all information is public to the blockchain suggests various challenges - varying from "transaction connectivity, crypto-key management, crypto-privacy resilience issues to quantum computing, chain data privacy, usage, interoperability or compliance of the provisions on confidentiality, such as the GDPR "(Bernal Bernabe et al., 2019). By default, all transactions that occur in Ethereum are visible to the public. Although system addresses are pseudonyms (Sas and Khairuddin, 2017), they may be decoded utilising centralised exchange information to identify customers and metadata (Neudecker and Hartenstein, 2017) (Victor, 2020). Because financial information is very sensitive to many people, privacy is a hot topic. In particular, consumers seek private transactions so that no unauthorised party can get data about consumers' financial activities. In addition, decentralisation, openness and protection of the integrity of blockchain technologies suggest challenges to compliance with confidentiality provisions (i.e. the right to be forgotten).

Nevertheless, various projects discuss these problems. Private transfers, according to Williamson, can be accomplished utilising various techniques (Aztec.network, 2021). For example, disconnection between the sender and the recipient of the tokens is possible when a contact party based on a smart contract is used (Tornado-cash.medium.com, 2019). Rollups enable customers to hide smart contracts, and Ernst & Young shares an open-source warehouse named Nightfall that utilises zk-snarks to do Ethereum transactions private (Medium.com, 2019). However, the overall confidentiality offering of public blockchains has serious remaining challenges to address. Bernabe et al. claim that consumers have the authority to execute anonymously in particular cases and that only by complying with this right can a blockchain support a truly confident model of identity (Bernal Bernabe et al., 2019).

Conclusion

In contrast to CeFi, DeFi offers inspiring possibilities, such as the power to build an open, transparent and unchanging financial infrastructure. Consisting of multiple extremely interoperable protocols and applications, all transactions may be checked by any individual and the data is easily accessible for analysis by users and researchers. On the other hand, the blockchain limits DeFi's transaction throughput, transaction confirmation latency, and privacy. Ultimately, DeFi and CeFi share the same goal: to provide customers with high-quality financial products and services and to boost the entire economy. To summarise, DeFi and CeFi each have their own set of advantages and disadvantages, and we cannot find a trivial way to combine the best of both systems. Therefore, we believe that these two distinct but intertwined financial systems will co-exist and improve each other. It is expected that CeFi and DeFi to co-exist, complement, strengthen and learn from each other's experiences, mistakes and innovations. CeFi and DeFi are already tightly intertwined (e.g., through centrally controllable stablecoins) and have jointly allowed the onboarding of a wider (e.g. technical) user demographic.

DeFi generally will be an attractive phenomenon that has huge and ever-growing potential. While the initial services posed issues such as payments and trading resolutions, progress has

been made to more modern products providing more sophisticated financial services. The Lego aspect reinforces this evolution even more. On the one hand, developers utilise smart contracts and decentralised decisions to create reliable forms of conventional financial tools. On the other hand, they build entirely new financial instruments that could not be executed without the main public blockchain. Atomic swaps, autonomous liquidity pools, decentralised stablecoins and flash loans are a few of the numerous illustrations that reveal the huge resources of this ecosystem. Based on the growing complexity, the management of these processes is becoming increasingly complex.

Although this system has big power, there are some dangers. The main challenges the system faces are scalability and safety. In particular, the existing scaling problems raise the question of whether Ethereum, as a modern DeFi platform, can cope with the growing demands. In addition, the term "decentralised" is misleading in some instances. Numerous protocols and applications utilise extrinsic information sources and distinguished administrator keys to manage the system, perform smart contract updates, or even accomplish urgent shutdowns. Despite this is not necessarily a problem, consumers should be aware that in many cases there is a great deal of trust. In addition, regulatory uncertainties need to be taken into account. In this regard, a solution for KYC is not available and, as a result, DeFi suffers from a lack of appropriate recognition as a valuable ecosystem of financial services in the eyes of the public. However, if these problems can be resolved, DeFi can bring a pattern change in the financial sector and conceivably promote a more stable and transparent financial infrastructure.

In general, it can be expected that the growth of DeFi can determine the growth of the blockchain sector in the forthcoming years, as it motivates decisions and enables people to access services when they are not offered by banks or other financial institutions.

References

Ammous, S. (2015). Economics Beyond Financial Intermediation: Digital Currencies' Potential for Growth, Poverty Alleviation and International Development. Ammous, Saifedean, pp. 19-50.

Aave.com. (2021). Aave – Open Source DeFi Protocol. [online] Available at: https://aave.com/ [Accessed 4 July 2021].

Abra.com. (2019). Abra Crypto Wallet: Buy Bitcoin, Earn Interest on Crypto. [online] Available at: https://www.abra.com/blog/crypto-bites-a-chat-with-ethereum-founder-vitalik-buterin/ [Accessed 13 March 2019].

Anjum, A., Sporny, M., Sill, A. (2017). Blockchain Standards for Compliance and Trust. – IEEE Cloud Computing, 4(4). doi: 10.1109/MCC.2017.3791019.

Antonopoulos, A. M. (2018). Mastering Ethereum: Building Smart Contracts And Dapps. Firts [Preprint].

Aztec.network. (2021). Aztec Protocol. [online] Available at: https://aztec.network/ [Accessed 4 July 2021].

Barnbridge.com. (2021). BarnBridge – A DeFi Risk Tokenizing Protocol. [online] Available at: https://barnbridge.com/ [Accessed 4 July 2021].

Basis.io, (2018). basis.io. [online] Available at: https:// https://www.basis.io/ [Accessed 13 December 2018].

Bernal Bernabe, J. et al. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. – IEEE Access. doi: 10.1109/ACCESS.2019.2950872.

Buterin and Vitalik. (2014). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Ethereum, (January).

Buterin, V. (2020). Ethereum Whitepaper | Ethereum.org. Ethereum.org.

Chen, Y., Bellavitis, C. (no date). Decentralised Finance: Blockchain Technology and the Quest for an Open Financial System.

Coingeek.com. (2020). CoinGeek: Bitcoin News & Blockchain Info. [online] Available at: https://coingeek.com/defi-project-origin-protocol-exploited-for-7-7-million/ [Accessed 17 November 2020].

Compound.finance. (2021). Compound Finance. [online] Available at: https://compound.finance/ [Accessed 4 July 2021].

Consensys.net. (2019). ConsenSys: Blockchain Technology Solutions | Ethereum .... [online] Available at: https://consensys.net/blog/news/2019-was-the-year-of-defi-and-why-2020-will-be-too/ [Accessed 5 December 2019].

Cryptoslate.com. (2020). CryptoSlate. [online] Available at: https://cryptoslate.com/another-day-another-hack-2m-in-dai-drained-from-ethereum-defi-app-akropolis/ [Accessed 13 November 2020].

Curve.fi. (2021). Curve.fi. [online] Available at: https://curve.fi/ [Accessed 4 July 2021].

Daian, P. et al. (2020). Flash boys 2.0: Frontrunning in decentralised exchanges, miner extractable value, and consensus instability. – In: Proceedings – IEEE Symposium on Security and Privacy. doi: 10.1109/SP40000.2020.00040.

Defipulse.com. (2021). DeFi Pulse – The Decentralised Finance Leaderboard. [online] Available at: https://defipulse.com/ [Accessed 4 July 2021].

Duneanalytics.com. (2021). Dune Analytics. [online] Available at: https://duneanalytics.com/ [Accessed 4 July 2021].

Erwig, A., Faust, S., Riahi, S., Stöckert, T. (2020). CommiTEE: An Efficient and Secure Commit-Chain Protocol using TEEs. IACR Cryptol. ePrint Arch., 1486.

European Commission. (2020). Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020), 593 final.

Flexa.network. (2021). Flexa. [online] Available at: https://flexa.network/ [Accessed 4 July 2021].

Gizmodo.com. (2020). Gizmodo | We come from the future. [online] Available at: https://gizmodo.com/garbage-crypto-product-dies-immediately-after-launch-1844718822 [Accessed 13 August 2020].

Grech, A., Camilleri, A. F. (2017). Blockchain in Education Luxembourg: Publications Office of the European Union, peDOCS.

Holotiuk, F., Pisani, F., Moormann, J. (2017). The Impact of Blockchain Technology on Business Models in the Payments Industry. – In: WI 2017 Proceedings.

Instadapp.io. (2021). Instadapp. [online] Available at: https://instadapp.io/ [Accessed 4 July 2021].

Leonhard, R. (2019). Decentralised Finance on the Ethereum Blockchain. – SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.3359732.

Liu, B., Szalachowski, P., Zhou, J. (2020). A first look into defi oracles. arXiv preprint arXiv:2005.04377.

Makerdao.com. (2021). MakerDAO | An Unbiased Global Financial System. [online] Available at: https://makerdao.com/en/ [Accessed 4 July 2021].

Medium.com. (2018). Medium – Where good ideas find you. [online] Available at: https://medium.com/wysker/crypto-exchanges-explained-549b42b47832 [Accessed 18 April 2018].

Medium.com. (2019). Medium – Where good ideas find you. [online] Available at: https://nodar.medium.com/introduction-to-decentralized-finance-aka-defi-ea4f12e6256d [Accessed 29 August 2019].

Medium.com. (2019). Medium – Where good ideas find you. [online] Available at: https://nodar.medium.com/introduction-to-decentralized-finance-aka-defi-ea4f12e6256d [Accessed 29 August 2019].

Medium.com. (2019). Medium – Where good ideas find you. [online] Available at: https://medium.com/@chaitanyakonda/nightfall-makes-token-transactions-on-ethereum-private-how-does-it-work-acf2ffd0aa7a [Accessed 10 June 2019].

Meiklejohn, S. et al. (2013). A fistful of bitcoins: Characterising payments among men with no names. – In: Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC. doi: 10.1145/2504730.2504747.

Moin, A., Sekniqi, K., Sirer, E.G. (2020). SoK: A Classification Framework for Stablecoin Designs. – In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi:10.1007/978-3-030-51280-4_11.

N. Janashia. Introduction to decentralised finance aka ‘defi’. https://medium.com/@Nodar/introduction-to-decentralized-financeaka-defiea4f12e6256d, 2019.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system, October 2008. Cited on.

Neudecker, T., Hartenstein, H. (2017). Could network information facilitates address clustering in bitcoin?. – In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi:10.1007/978-3-319-70278-0_9.

News.bitcoin.com. (2020). Bitcoin News - Bitcoin.com. [online] Available at: https://news.bitcoin.com/defi-token-exposed-as-pump-and-dump-scam-in-leaked-telegram-chat/ [Accessed 28 September 2020].

Nexusmutual.io. (2021). Nexus Mutual | A decentralised alternative to insurance. [online] Available at: https://nexusmutual.io/ [Accessed 4 July 2021].

Qin, K. et al. (2021). Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. doi:10.1007/978-3-662-64322-8_1.

Sas, C., Khairuddin, I. E. (2017). Design for trust: An exploration of the challenges and opportunities of bitcoin users. – In: Conference on Human Factors in Computing Systems – Proceedings. doi:10.1145/3025453.3025886.

S. Shoeb. Decentralization disrupting the finance ecosystem. https://medium.com/datadriveninvestor/compound-vs-nuo-vs-dharmavs- maker-whichone-is-the-best-d85d5d614bb1.

Schär, F. (2020). Decentralised Finance: On Blockchain- and Smart Contract-based Financial Markets. – SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.3571335.

Schilling, L., Uhlig, H. (2019). Some simple bitcoin economics. – Journal of Monetary Economics, p. 106. doi:10.1016/j.jmoneco.2019.07.002.

Synthetix.io. (2021). Synthetix. [online] Available at: https://www.synthetix.io/ [Accessed 4 July 2021].

Theblockcrypto.com. (2020). The Block – The First and Final Word in Digital Assets. [online] Available at: https://www.theblockcrypto.com/post/79061/yfi-eminence-defi-protocol-exploited [Accessed 29 September 2020].

Tornado-cash.medium.com. (2019). Tornado.cash [online] Available at: https://tornado-cash.medium.com/introducing-private-transactions-on-ethereum-now-42ee915babe0 [Accessed 7 Aug 2019].

Uniswap.org. (2021). Uniswap. [online] Available at: https://uniswap.org/ [Accessed 4 July 2021].

Victor, F. (2020). Address Clustering Heuristics for Ethereum. – In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi:10.1007/978-3-030-51280-4_33.

Winzer, F., Herd, B., Faust, S. (2019). Temporary censorship attacks in the presence of rational miners. – In: Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019. doi: 10.1109/EuroSPW.2019.00046.

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. – Ethereum Project Yellow Paper.

Wüst, K., Gervais, A. (2017). Do you need a Blockchain?. IACR Cryptology ePrint Archive [Preprint], (i).

Xdaichain.com. (2021). xDai - xDai. [online] Available at: https://www.xdaichain.com/ [Accessed 4 July 2021].

Xu, L. et al. (2017). Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain. – In: BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, co-located with ASIA CCS 2017. doi: 10.1145/3055518.3055527.

Yeung, K. (2019). Regulation by blockchain: The emerging battle for supremacy between the code of law and code as law. – Modern Law Review, 82(2). doi: 10.1111/1468-2230.12399.