

DeFi-ning DeFi: Challenges & Pathway

Hendrik Amler
PolyCrypt
Germany
hendrik@polycry.pt

Lisa Eckey
Deutsche Telekom Security
Germany
lisa.eckey@crisp-da.de

Sebastian Faust
Chair of Applied Cryptography
TU Darmstadt, Germany
sebastian.faust@tu-darmstadt.de

Marcel Kaiser
Frankfurt School Blockchain Center
Frankfurt School of Finance
and Management, Germany
Marcel@polycry.pt

Philipp Sandner
Frankfurt School Blockchain Center
Frankfurt School of Finance
and Management, Germany
philipp.sandner@fs-blockchain.de

Benjamin Schlosser
Chair of Applied Cryptography
TU Darmstadt, Germany
benjamin.schlosser@tu-darmstadt.de

Abstract—The decentralized and trustless nature of cryptocurrencies and blockchain technology leads to a shift in the digital world. The possibility to execute small programs, called smart contracts, on cryptocurrencies like Ethereum opened doors to countless new applications. One particular exciting use case is decentralized finance (DeFi), which aims to revolutionize traditional financial services by founding them on a decentralized infrastructure. We show the potential of DeFi by analyzing its advantages compared to traditional finance. Additionally, we survey the state-of-the-art of DeFi products and categorize existing services. Since DeFi is still in its infancy, there are countless hurdles for mass adoption. We discuss the most prominent challenges and point out possible solutions. Finally, we analyze the economics behind DeFi products. By carefully analyzing the state-of-the-art and discussing current challenges, we give a perspective on how the DeFi space might develop in the near future.

Index Terms—blockchain, finance, contracts, distributed ledgers

I. INTRODUCTION

Blockchain and distributed ledger technology (DLT) have gained huge popularity since the development of Bitcoin [1] over a decade ago. Beyond simple financial transactions, many DLTs support scripts for their transactions, allowing users to define complex rules and conditions for payments. Some blockchains even allow payments to depend on the execution of Turing-complete programs, so-called smart contracts [2]. A plethora of traditionally centralized financial instruments are now being deployed and used on distributed blockchain systems using smart contracts. These financial services are often referred to as *Decentralized Finance (DeFi)*.

The fundamental innovation of DeFi is similar to blockchains: reducing trust by replacing centralized platforms with a decentralized system. The resulting system is considered trustless. Additionally, DeFi systems are open to anyone. In particular, this means individuals can also take on roles which were traditionally in the hands of banks. As DeFi products are built on smart contracts, multiple DeFi products can be composed by letting smart contracts interact. This allows developers to build flexible and powerful tools. This connectivity of DeFi is often called *financial Lego*. Of course,

composability also leads to more complexity for users and developers and has resulted in spectacular security breaches. This is particularly dangerous because, unlike in centralized systems, there is no way to undo transactions. In Ethereum, which is the largest DeFi ecosystem at the time of writing, smart contracts cannot be changed easily after deployment and funds sent to them will be processed as programmed, which is not always as intended by users. There are countless examples of faulty smart contracts. Despite these risks, the demand for DeFi services is unbroken, reaching new highs in Q3 2020.

A. Contribution

We provide a definition for DeFi and discuss its advantages in comparison to traditional finance in Section II. Moreover, we categorize DeFi products to give a broader understanding of how DeFi products are currently used in practice. Additionally, we provide an overview of current governance and economic topics in the field in Section III.

Lastly, we investigate the main challenges and possible solutions for DeFi products in a comprehensive way in Section IV.

A more detailed analysis can be found in the full version [3].

B. Related Work

Concurrently to our work, Harvey et al. [4] surveyed financial infrastructures including DeFi. While we analyze the DeFi ecosystem as a whole, another line of work focuses on single aspects. Moin et al. [5], Klages-Mundt et al. [6] and Clark et al. [7] study the fundamentals of stablecoins which play an important role in DeFi protocols. Pernice et al. [8] analyze the stabilization of cryptocurrencies and systematically survey existing DeFi products. Daian et al. [9] and Qin et al. [10] study the security aspect of DeFi and show real-world attacks.

II. POTENTIAL OF DEFI

Decentralized finance represents a whole ecosystem of financial services realized through smart contracts deployed on public distributed ledgers. Instead of relying on traditional, providers of financial services, which are accompanied by high costs, lengthy processes and a lack of transparency, DeFi realizes decentralized financial services. Through the employment of publicly available protocols and decentralized apps (dApps), DeFi enables individuals to play both sides of financial transactions, democratizing financial instruments.

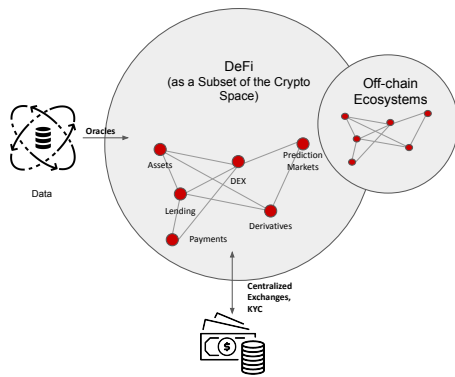


Fig. 1. Overview of the DeFi landscape

A. Advantages of the DeFi Ecosystem

Next, we list the main advantages of DeFi services in comparison to traditional financial systems.

Permissionless: Public blockchains are designed to be open, meaning that they do not specify access rules and anyone can interact with them [11]. DeFi applications built on public blockchains inherit these properties by default.

Trustless: While distributed ledgers do not rely on a single operator as a trusted agent, they distribute trust across a network of nodes instead [12].

Transparent: Most public distributed ledgers provide transparency by default since all transactions stored in the blockchain are publicly visible at any time.

Interconnected: Complex applications, including auctions, voting and trading, can be built with smart contracts. Their features can be called by users and smart contracts, making it possible to easily connect, stack or combine existing applications without additional programming efforts.

Decentrally governed: Not restricted to the DeFi space but highly prevalent in it is the aspect of turning smart contracts into decentralized autonomous organizations (DAOs). By enabling the community to suggest legislation and vote based on their stake in the project, governance is distributed.

Enabling self-sovereignty: As no central authority controls and organizes access to the decentralized environment, users themselves manage their data and custody of their funds.

B. Overview of Financial Services

We classify existing DeFi applications into six categories: lending platforms, asset handling platforms, decentralized exchanges (DEXes), derivative services, payment networks and prediction markets. Fig. 1 shows an abstract illustration of the DeFi landscape containing these interconnected categories. The connection to the outside of the DeFi space, i.e., real-world data and fiat money, is realized via oracles and centralized exchanges. Inserting live data into a blockchain creates a number of challenges that are discussed in Section IV-C.

While more topics are emerging, we focus on the most important categories.¹ For the sake of compactness, we outline

¹The above-mentioned categories pose classification guidelines, as many aspects of DeFi are still subject to change. Moreover, many DeFi services may be associated with more than one or even additional categories.

three of these categories in the following.²

Lending Platforms: Decentralized lending services offer loans to businesses or individuals using smart contracts as intermediaries, negotiators and for setting interest rates according to supply and demand.

Decentralized Exchanges (DEXes): Services that focus on decentralized cryptocurrency and token exchange are often classified as DEXes. DEXes work similar to a stock exchange, but instead of being run by a central provider, the exchange is operated by a smart contract deployed on, e.g., Ethereum.

Derivative Services: DeFi derivatives build on smart contracts that derive value from the performance of an underlying entity such as bonds, currencies, or interest rates. Tokenized derivatives can be created without third parties and by-design prevent malicious influence.

III. ECONOMICS AND GOVERNANCE

A. Decentralized Governance

Major protocols and exchanges use decentralized governance to update their policy regularly, allowing stakeholders to vote. The voting power depends on the number of (tradable) governance tokens held. An airdrop (i.e., transfer of tokens to eligible wallets) by Uniswap, for example, benefited early users. Any owner of the token is eligible to vote. Not only exchanges use this model, but also the lending platform Maker. The difference is that the Maker governance token (MKR) is deflationary due to burning, while the Uniswap governance token (UNI) has inflationary properties in the midterm.

These various approaches lead to different effects: while a UNI holder loses relative voting power if they are not actively mining the tokens by providing liquidity, MKR holders tend to become more influential over time without active interaction with the protocol. Both dynamics make sense for smart contracts as they serve their respective use case: MKR tokens need to be burned to stabilize DAI, and Uniswap aims to gradually become more decentralized by allowing users to mint.

Our analysis of how token concentration across wallets has changed can be found in the full version of this paper [3]. Furthermore, [13] provided a thorough analysis of voting power concentration using similar approaches.

B. Economics

The DeFi space has seen rapid growth in 2020. In the time from November 2018 to March 2021, the locked value in DeFi protocols has increased close to 220 times to \$41.06B. This growth in locked up value (collaterals and lent DAI) stems from reinvested gains, increased Ether valuations and from a larger number of users.³

It is assumed that DeFi significantly influenced the transaction cost within the Ethereum network. Consequently, the incentive to avoid unnecessary transactions has increased. Especially automated trading protocols and DEX arbitrageurs caused the increase in the number of transactions.

While the metrics of this space are notable, they are shy of conventional financial markets. The DeFi space is still

²A full list and further details can be found in the full version of this paper [3].

³At the time of writing, over 1.7 million unique DeFi addresses have been counted using data from Dune Analytics [14]. This number is an overestimation as users can create multiple wallets.

novel, unregulated and taxation for users remains unclear, negatively impacting the growth of the system. It can be expected that increased institutional attention will be laid on the decentralization of the financial sector in the coming years. Especially once central bank digital currencies (CBDCs) become available, compatible and scalable DeFi DApps could have the potential to disrupt the financial sector.

IV. CHALLENGES

This section presents critical challenges for the DeFi space face and provides potential solutions. We refer to the full version of this paper for more details [3].

A. Security

We identify three aspects of DeFi products that require special attention in terms of security: smart contract vulnerabilities, infrastructural risk and interdependence weaknesses.

First, DeFi products are built upon smart contracts dealing directly or indirectly with user funds. Since applications with more locked assets are more attractive to attack, smart contract developers must put effort into programming contracts without vulnerabilities for DeFi. Additional security audits from external parties may increase the trust in the correctness of a contract. The past showed the massive impact of programming bugs in smart contracts, e.g., on the origin protocol [15].

Second, the underlying infrastructure may have additional influences on the product, which needs to be considered when designing application-specific security mechanisms. For instance, the limited throughput of the Ethereum blockchain led to a congestion of the network in 2020. Suppose a contract makes use of timeouts to ensure timely interaction by the participants a congested network may result in users missing their timeouts since valid transactions from honest users might not be recorded in time [16].

Third, because of the Lego aspect of DeFi (see Section II), designing new protocols for the DeFi space requires special consideration. The security of a single protocol cannot be analyzed in a standalone model; influences of other protocols also need to be taken into account. We show this aspect by highlighting frontrunning attacks, which were analyzed by Daian et al. [9]. The term frontrunning comprises all scenarios where one party tries to get her transaction recorded before a competing transaction. Another attack exploiting interdependence weaknesses was presented by Qin et al. [10].

B. Limited Scalability

Blockchain technology and its applications suffer from limited transaction throughput, which is often viewed as the main hurdle for mass adoption of this technology [17]. The underlying reason is that blocks in the ledger only have limited space shared by transactions, smart contract deployments and contract function invocations.

Ethereum can be considered the primary choice for DeFi applications and especially suffers from limited scalability as the blockchain cannot handle the growing number of users and emerging DeFi applications.

The challenge of limited scalability is tackled on two different layers. Layer-1 solutions aim for improving the consensus mechanism of blockchain technologies [18]. Approaches include changing the consensus mechanism like in EOS [19] or

applying sharding techniques where the state of the blockchain is split into several units called shards (see [20] and [21]). In contrast to Layer-1 solutions, Layer-2 techniques tackle the application layer's scalability issue without requiring any changes to the underlying consensus mechanism. Solutions tailored towards the challenges of DeFi use cases where the execution of complex smart contracts is required, utilize zkRollups or optimistic rollups [22], [23].

C. Oracles

Many DeFi products rely on external information like exchange rates, which is provided by so called oracles. Since the data originating from these oracles impact the behavior of smart contracts and users, the challenges posed by transferring external data on-chain is a major concern. In particular, the security of these DeFi products is based on the reliability, accuracy and correctness of the provided information from oracles. Therefore, oracles are evaluated based on their transparency, accountability and the required level of trust.

We elaborate on the usage of oracles by describing how the Maker project addresses some challenges by combining inputs from multiple sources in the full version of this paper [3]. Liu and Szalachowski [24] conducted a study of DeFi oracles presenting large-scale measurements about different price metrics. Moreover, the authors propose recommendations for oracle solutions.

D. Regulation

Most existing regulatory concepts are yet primarily concerned with the classification of tokens for taxation purposes. The legal status of the entire ecosystem and generated income is not clearly defined. Questions about the potential for illicit usages arise. There is a significant gap between governance and external regulation to fill. Moreover, the lack of know your customer (KYC) processes in DeFi ecosystems makes it harder for regulators to accept it. As a consequence, regulators are confronted with the great challenge of not inhibiting innovation when regulating DeFi. Yeung (2019) [25] states that a balance between legal and technical code sustains interactions of different dimensions (economic, political, social).

In September of 2020, the European Commission presented a draft for the regulation of "crypto assets" which is expected to be in force by 2023. The regulation "Markets in Crypto-assets" ("MiCA"), which is directly applicable for all European member states, describes the most extensive regulation of digital assets to date. While the proposal covers most types of crypto assets and categorizes them, DeFi tokens are not explicitly dealt with. The DAI stablecoin can be classified as a asset-referenced token [26]. It is likely that smart contracts in the DeFi space can be classified as crypto asset service providers at some point. However, conclusive legal research has to be performed in order to clarify this relationship further.

E. On- And Offramping

On- and offramps refer to the methods to exchange traditional assets for crypto-assets and vice versa. Centralized exchanges are based on trust in an intermediary, require authentication via KYC practices, have limited scalability, suffer from security issues, process transactions off-chain and charge significant fees [27]. Many of these shortcomings are

equivalent to limitations that traditional banks face. The leading centralized exchanges are Coinbase, Binance and Kraken. To enable seamless on- and offramps, these companies must evolve significantly to satisfy all customers' requirements.⁴

F. Privacy

The fact that all data is public on the blockchain poses several challenges - ranging from "transaction linkability, crypto-key management, issues with crypto-privacy resistance to quantum computing, on-chain data privacy, usability, interoperability, or compliance with privacy regulations, such as the GDPR" [28].⁵ Since financial data is highly sensitive for individuals, privacy is a relevant topic. The openness and integrity protection of blockchain technologies pose challenges for compliance with privacy regulations (e.g. the right to be forgotten).

However, several projects address these issues. Private transfers (as described in [29]) can be achieved using several techniques. For example, disconnecting the link between the sender and recipient of tokens is possible when using a mixer based on smart contracts [30]. Rollups allow users to hide smart contracts [31] and Ernst & Young shared an open-source repository (Nightfall) that uses zk-snarks to make Ethereum transactions private [32]. Bernabe et al. [28] argue that it is the users' right to act anonymously in specific situations and that only by adhering to this right, blockchains can provide a genuinely self-sovereign identity model.

V. SUMMARY

DeFi as a whole will remain an interesting phenomenon and has lots of potential, growing continuously. The major challenges in the near future remain to be scalability and security. Moreover, regulatory uncertainties need to be solved. A solution for KYC is not yet available and as a consequence, DeFi lacks proper recognition as a valuable financial service ecosystem in the public eye.

All in all, it can be expected that DeFi's growth can co-determine the growth of the blockchain sphere within the coming years as it motivates solutions and gives individuals the opportunity to access services when unbanked.

VI. ACKNOWLEDGMENTS

We want to thank Leon Erichsen whose research helped us gaining an initial perspective. This work was partly funded by the projects iBlockchain and ProChain (grant nr. 16KIS0902 and 16KIS1015 by the German Federal Ministry of Education and Research), by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 – 236615297 (Project S7), and by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

⁴Note: because USDT is the primary stablecoin in use, it is a de facto central gateway. This introduction of counterparty risk in the decentralized financial systems can have consequences: accessibility for many decreases and the offramping becomes significantly harder, which might cause the ecosystem to halt its growth and possibly revert it until a suitable replacement is found.

⁵Although the system's addresses are pseudonyms, they are decodable using information from centralized exchanges about client identification and other metadata.

REFERENCES

- [1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.
- [2] V. Buterin et al. Ethereum whitepaper. <https://ethereum.org/en/whitepaper/>.⁶
- [3] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner, and B. Schlosser. Defi-ning defi: Challenges & pathway. *CoRR*, abs/2101.05589, 2021.
- [4] C. R. Harvey, A. Ramachandran, and J. Santoro. Defi and the future of finance. <https://ssrn.com/abstract=3711777>.
- [5] A. Moin, K. Sekniqi, and E. G. Sirer. Sok: A classification framework for stablecoin designs. In J. Bonneau and N. Heninger, editors, *Financial Cryptography and Data Security*, pages 174–197, 2020.
- [6] A. Klages-Mundt, D. Harz, L. Gudgeon, J. Liu, and A. Minca. Stablecoins 2.0: Economic foundations and risk-based models. In *Conference on Advances in Financial Technologies*, pages 59–79. ACM, 2020.
- [7] J. Clark, D. Demirag, and S. Moosavi. Demystifying stablecoins. *ACM Queue*, 18(1):39–60, 2020.
- [8] I. G. A. Pernice, S. A. Henningsen, R. Proskalovich, M. Florian, H. Elendner, and B. Scheuermann. Monetary stabilization in cryptocurrencies - design approaches and open questions. In *Crypto Valley Conference on Blockchain Technology*, pages 47–59. IEEE, 2019.
- [9] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *IEEE Symposium on Security and Privacy*, pages 910–927. IEEE, 2020.
- [10] K. Qin, L. Zhou, B. Livshits, and A. Gervais. Attacking the defi ecosystem with flash loans for fun and profit. *CoRR*, abs/2003.03810, 2020.
- [11] S. Shueb. Decentralization disrupting the finance ecosystem. <https://medium.com/datadriveninvestor/compound-vs-nuo-vs-dharma-vs-maker-whichone-is-the-best-d85d5d614bb1>.⁶
- [12] A. Anjum, M. Sporny, and A. Sill. Blockchain standards for compliance and trust. *IEEE Cloud Computing*, 4(4):84–90, 2017.
- [13] J. R. Jensen, V. von Wachter, and O. Ross. How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions, 2021.
- [14] Dune analytics. <https://duneanalytics.com/>.⁶
- [15] Defi project origin protocol exploited for \$7.7 million. <https://coingeek.com/defi-project-origin-protocol-exploited-for-7-7-million/>.⁶
- [16] F. Winzer, B. Herd, and S. Faust. Temporary censorship attacks in the presence of rational miners. In *European Symposium on Security and Privacy Workshops*, pages 357–366. IEEE, 2019.
- [17] Crypto bites: Chat with ethereum founder vitalik buterin - youtube. https://www.youtube.com/watch?v=u-i_mTWL-FI&feature=youtu.be.⁶
- [18] L. M. Bach, B. Mihaljevic, and M. Zagar. Comparative analysis of blockchain consensus algorithms. In *International Convention on Information and Communication Technology, Electronics and Microelectronics*, pages 1545–1550, 2018.
- [19] Eosio - blockchain software architecture. <https://eos.io/>.⁶
- [20] The zilliqa technical whitepaper. <https://docs.zilliqa.com/whitepaper.pdf>, August 2017.
- [21] Elrond. <https://elrond.com/assets/files/elrond-whitepaper.pdf>, June 2019.
- [22] Loopring. <https://loopring.io/>.⁶
- [23] IDEX. <https://idex.io/>.⁶
- [24] B. Liu and P. Szalachowski. A first look into defi oracles. *CoRR*, abs/2005.04377, 2020.
- [25] K. Yeung. Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law. *The Modern Law Review*, 82(2):207–239, 2019.
- [26] E. Commission. Proposal for a regulation of the european parliament and of the council on markets in crypto-assets (mica), November 2020.
- [27] F. Koenig. Crypto exchanges explained. <https://medium.com/wysker/crypto-exchanges-explained-549b42b47832>.⁶
- [28] J. B. Bernabé, J. L. Cánovas, J. L. H. Ramos, R. T. Moreno, and A. F. Skarmeta. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7:164908–164940, 2019.
- [29] D. Z. J. Williamson. The aztec protocol. <https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf>.⁶
- [30] T. Cash. Introducing private transactions on ethereum now! <https://medium.com/@tornado.cash/introducing-private-transactions-on-ethereum-now-42ee915babe0>, August 2019.⁶
- [31] Optimism. <https://medium.com/ethereum-optimism/optimism-cd9bea61a3ee>.⁶
- [32] C. Konda, M. Connor, D. Westland, Q. Drouot, and P. Brody. Nightfall.

⁶(Accessed on 03/29/2021)