5 DeFi risks and challenges

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

Technical Risks

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

Consequently, there have been a wide range of DeFi hacks where several million USD of value have been stolen and/or lost in different projects[3]. Potential remedies for code bugs and technical failures could be third party audits and insurance schemes, regulation (see regulation subchapter) in the form of necessary risk management procedures, capital buffers, and consumer protection. Alternatively, transparent and formalized processes of »good governance« within the DeFi protocols, which can quickly freeze the smart contract, update the code, or even undo certain transactions in extreme cases, such as the DAO fork refund 2018[4].

Apart from risks regarding smart contract bugs and inaccuracies, technical risks regarding the underlying blockchain protocol (layer 0) also have to be taken seriously. Nearly all relevant DeFi projects are built on top of the Ethereum blockchain. In times of high usage, Ethereum has experienced a few clogging issues on its blockchain. If the network gets congested, a transaction can remain in a pending state, which ultimately results in market inefficiency and information delays. Those technical scalability problems are closely related to liquidity risks (see liquidity subchapter). Given the current bottlenecks in terms of throughput, it is highly questionable whether DeFi is viable on Ethereum, especially if Ethereum experiences a further user base growth. In short, DeFi is thus highly dependent on a successful Ethereum 2.0 update, which could solve these technical issues, but is expected to take at least several more years[5].

Other smart contracts offering blockchain platforms (EOS, Tezos etc.) could also take over Ethereum's leading role in the DeFi space, but currently face other problems such as insufficient decentralization (see centralization subchapter) or a missing developer/community base. Part of the reason why Ethereum is currently the leading platform is because its high usage leads to

3 ↗https://www.coindesk.com/defi-project-bzx-exploited-for-second-time-in-a-week-loses-630k-in-ether
↗https://www.coindesk.com/defi-dforce-refund-users-after-25m-hack

4 ↗https://www.google.com/search?q=dao+fork+undone&rlz=1C1GGRV_enDE781DE781&oq=dao+fork+undone&aqs=chrome..69i57.7322j0j7&sourceid=chrome&ie=UTF-8

5 ↗https://www.coinspeaker.com/buterin-ethereum-2-next-5-10-years/