Fraunhofer
FIT

Branch Business & Information
Systems Engineering,
Fraunhofer Institute for Applied
Information Technology FIT

Decentralized Finance (DeFi)

Foundations, Applications, Potentials, and Challenges

Decentralized Finance (DeFi)

Foundations, Applications, Potentials, and Challenges

Authors

Vincent Gramlich, Marc Principato, Benjamin Schellinger, Johannes Sedlmeir, Julia Amend, Jan Stramm, Till Zwede, Prof. Dr. Jens Strüker, and Prof. Dr. Nils Urbach

The Branch Business & Information Systems Engineering of Fraunhofer FIT, located in Augsburg and Bayreuth, has proven expertise at the interface of Financial Management, Information Management, and Business & Information Systems Engineering. The ability to combine methodological know-how at the highest scientific level with a customer-focused and solution-oriented way of working, is our distinctive feature.

Fraunhofer Institute for Applied Information Technology FIT
Branch Business & Information Systems Engineering
Wittelsbacherring 10
95444 Bayreuth

Acknowledgement

We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their support of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" that made this paper possible.

Sponsored by

Bavarian Ministry of Economic Affairs,
Regional Development and Energy

We also thank Martin Brennecke, Bjarne Huuck, Felix Paetzold, and Vincent Schlatt for their support in administration, form, language review, illustrations, and content for this paper.

Disclaimer

This study has been prepared by the Fraunhofer Institute for Applied Information Technology FIT to the best of its knowledge and belief, using professional diligence. Fraunhofer FIT, its legal representatives, and/or vicarious agents do not guarantee that the contents of this study are secure, completely usable for specific purposes, or otherwise free of errors. The use of this study is entirely at the user's own risk. In no event shall Fraunhofer FIT, its legal representatives, and/or agents be liable for any damages whatsoever, whether directly or indirectly, arising out of or in connection with the use of this study.

Recommended citation

Gramlich, V., Principato, M., Schellinger, B., Sedlmeir, J., Amend, J., Stramm, J., Zwede, T., Strüker, J., and Urbach, N. (2022): Decentralized Finance (DeFi) – Foundations, Applications, Potentials, and Challenges. Branch Business & Information Systems Engineering of Fraunhofer FIT.

Image sources

© https://www.stock.adobe.com/, https://www.shutterstock.com/

DeFi enables innovative financial services and offers efficiency gains via modularity and openness, but it also leads to enormous legal, technical, and socio-economic challenges that need to be resolved.

Preface

Bitcoin and other cryptocurrencies built on blockchains have increasingly attracted investors in recent years. Motivated by the opportunities of this technology, blockchain-based applications in various sectors have also been explored. Yet, so far, finance-related applications have arguably remained the most advanced and relevant area of blockchain usage. The resulting financial ecosystem based on blockchains as infrastructure is often referred to as ***decentralized finance (DeFi)***. DeFi integrates not only basic payment functionalities, but also provides highly complex applications that interconnect different building blocks and services. These features result in the creation of an open, trustless, composable, and permissionless financial ecosystem. Protocols built on blockchains, i.e., smart contracts, facilitate automation and highly customizable DeFi applications. Thus, smart contracts enable a wide range of financial services such as digital assets (e.g., stablecoins and derivatives), participation mechanisms (e.g., governance in decentralized autonomous organizations (DAOs)), and investment opportunities (e.g., non-fungible tokens (NFTs) and fractional ownership).

Proponents of DeFi argue that removing central entities in the value chain of traditional finance (TradFi) improves access to financial services, lowers transaction costs, increases flexibility, and drives innovation. However, the nascent stage of DeFi still poses major risks and challenges: Regulatory bodies are looking for means to prevent money laundering and to hold entities accountable for misbehavior. Also, the transparent nature of blockchains raises questions regarding compliance with data protection and related privacy regulations. Bridging cryptocurrencies, DeFi-based transactions, and the real world is another multi-faced challenge. Furthermore, security and scalability issues hamper the development of promising applications. The current scalability issues, for example, cause high transaction costs that make DeFi less attractive or unusable for non-affluent users, undermining the value proposition of DeFi.

Understanding DeFi's potentials and challenges is a crucial prerequisite to seize business opportunities early on. In addition, it is imperative to educate investors, policy-makers, and users about the principles of DeFi. Moreover, innovation from DeFi has arguably inspired many other sectors. Thus, the technical innovations in DeFi can facilitate decentralized applications (DApps) in various domains, e.g., payments using central bank digital currencies (CBDCs) or verifiable supply chains. Blockchain and smart contracts can allow companies to freely capitalize on composable, trustless, and permissionless DeFi protocols to build and offer innovative products and services.

The goal of our study is to shed light on DeFi and provide experts and non-experts with the required knowledge to comprehensively understand this emerging phenomenon. In addition, we discuss potentials, but also existing challenges of DeFi and present solutions and measures for risk mitigation. We hope readers enjoy this study and welcome questions, discussions, and suggestions for improvement.

©Hochschule Fresenius/ John M. John

Prof. Dr. Jens Strüker

Professor of Information Systems
and Digital Energy Management,
University of Bayreuth

Head of Fraunhofer Blockchain-Lab,
Branch Business & Information Systems
Engineering of Fraunhofer FIT

jens.strueker@fit.fraunhofer.de

©Björn Seitz – kontender.Fotografie

Prof. Dr. Nils Urbach

Professor of Information Systems,
Digital Business and Mobility,
Frankfurt University of Applied Sciences

Head of Fraunhofer Blockchain-Lab,
Branch Business & Information Systems
Engineering of Fraunhofer FIT

nils.urbach@fit.fraunhofer.de

Glossary

AML	anti-money laundering
AMLD	Anti-Money Laundering Directive
AMM	automated market maker
API	application programming interface
BaFin	German Federal Financial Supervisory Authority
CARF	Crypto-Asset Reporting Framework
CBDC	central bank digital currency
CeDeFi	centralized decentralized finance
CEX	centralized exchange
CFT	countering the financing of terrorism
CFTC	Commodity Futures Trading Commission
DAO	decentralized autonomous organization
DApp	decentralized application
DeFi	decentralized finance
DEX	decentralized exchange
DLT	distributed ledger technology
DSP	direct stock purchase
ERC	Ethereum request for comments
EU	European Union
FATF	Financial Action Task Force on Money Laundering
FEC	Federal Election Commission
FinCEN	Financial Crimes Enforcement Network
GDPR	General Data Protection Regulation
IAS	International Accounting Standard
ICO	initial coin offering
IDO	initial decentralized exchange offering
IEO	initial exchange offering
IFRS	International Financial Reporting Standards
IPO	initial public offering
KYC	know your customer
L2	layer 2
MEV	miner extractable value
MiCA	markets in crypto assets
NFT	non-fungible token
OECD	Organisation for Economic Co-operation and Development
P2P	peer-to-peer
PoA	proof of authority
PoS	proof of stake

PoW	proof of work
SEC	Securities Exchange Comission
TIA	things in action
TIP	things in possession
TradFi	traditional finance
TVL	total value locked
TVTG	Tokens and Trustworthy Technologies Service Providers Law
VASP	virtual asset service provider
ZKP	zero-knowledge proof

Contents

1 Introduction

1 Introduction

Since the inception of Bitcoin in 2008, financial markets have seen a sharp increase in market capitalization for various blockchain-based assets in recent years. Yet, Bitcoin still represents the most popular cryptocurrency, with a market capitalization amounting to approximately USD 370 billion as of mid 2022. The recent phenomenon of blockchain-based applications such as non-fungible tokens (NFTs) and the emergence of decentralized finance (DeFi) have also contributed to the mushrooming of digital assets. In particular, DeFi has experienced tremendous momentum, with cryptocurrency investments locked to the Ethereum blockchain exceeding USD 100 billion by the end of 2021 (see Figure 1). DeFi has witnessed a rapid increase in market value in 2021, accompanied by a growing user base and the emergence of new, innovative use cases. Against this backdrop, we believe that exploring and developing a comprehensive understanding of DeFi marks a worthwhile endeavor.

Although blockchains have long been closely associated with financial applications, today applications have evolved into a more general multipurpose area. With the advent of the Ethereum blockchain, it was possible for the first time to execute arbitrary, user-defined programming logic (Buterin, 2014). These pieces of code, called “smart contracts”, built and run on blockchains, provide new opportunities for the development of more advanced financial applications and infrastructures. As a result of these innovative features, a new ecosystem has emerged, referred to as DeFi. It is also conceived to be a movement to develop decentralized financial applications that do not depend on a distinguished central authority and therefore resist manipulation and censorship to a certain extent (CoinGecko, 2020). Proponents of such non-institutional financial services claim that DeFi can aid in improving financial inclusion, thereby reducing poverty, inequality, government censorship, and increasing economic growth globally. In addition, the underlying DeFi protocols promise to automate processes, specifically across different organizations (Fridgen et al., 2018a), offering the opportunity for higher transaction speed. Since the code is generally open source and cannot be altered beyond the established rules once it is deployed, trust can be placed in the integrity and functionality of DeFi applications. Moreover, the modular components of DeFi aim to improve the building and linking of financial applications without the need for access to bank-specific application programming interfaces (APIs). Beyond these potentials, there are further developments around technologies that do not yet have a direct relation to DeFi but may have strong interactions with it in the future. For example, digital identities based on asymmetric cryptography allow persons, organizations, and machines to provide machine-verifiable information (Sedlmeir et al., 2021b; Strüker et al., 2021) and, thus, may facilitate a bridge between regulated domains and DeFi (Sedlmeir et al., 2022).

Nevertheless, there are still great challenges that need to be addressed to unleash DeFi’s potential to the economy and society. For instance, there have been multiple attacks owing to security gaps in DeFi applications, often by targeting users through phishing attacks, hacking or by abusing flaws in smart contract code. In addition, there have been a lot of attempts to commit financial fraud through initial coin offering (ICO) scams, pump and dump schemes, and other activities that traditional financial markets have inhibited through regulation over the last centuries. Regulators are also concerned that DeFi may undermine financial stability and put consumers at risk (Financial Stability Board, 2022). Another challenge of DeFi is caused by the inherent transparency of blockchain, which can be problematic with respect to data protection or antitrust compliance requirements. Worse, transparency grants miners an undue advantage by allowing them to make (arguably) illegitimate profits by front-running and other activities that would be prevented in regulated markets. In general, the large number of unregulated entities involved not only make it challenging to compensate investors for losses following such events. The pseudonymity

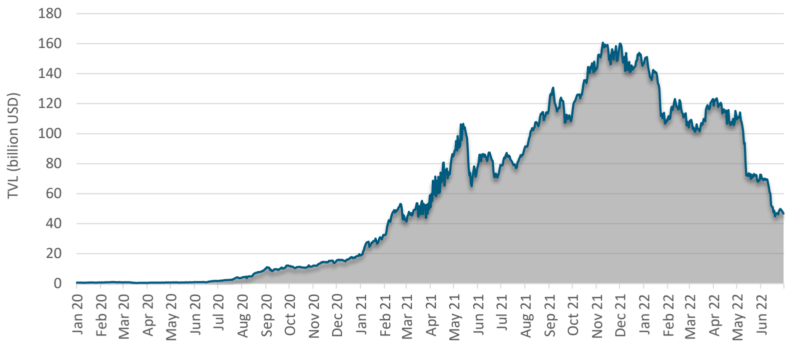


Figure 1: Total value locked in DeFi on Ethereum (data retrieved from DeFiLlama (2022)).

of accounts in DeFi can also make it difficult to comply with anti-money laundering (AML) and countering the financing of terrorism (CFT) regulation. As they represent distributed and decentralized systems that are synchronized to a consistent state, blockchains typically require multiple devices to perform the same operation in order to ensure and uphold data integrity. This leads to a lower processing capacity in comparison to centralized databases. Hence, from a technical point of view, the challenge is to find solutions to avoid congestion, high transaction latencies, and transaction costs that arise from scalability issues.

Despite recent developments, the DeFi ecosystem is currently still in its infancy. However, DeFi components are already being connected to central systems operated by traditional finance (TradFi) institutions and marketplaces. According to the "Protocol Sink Thesis", open, permissionless DeFi applications will increasingly converge with centralized entities in the future (Hoffman, 2020). It also states that the DeFi ecosystem is the first financial system that provides settlement assurances enabled by the underlying technology-stack instead of relying on laws or governments to enforce its rule. Thus, these trustless, permissionless, and unbiased protocols will "sink to the bottom" and become the technical infrastructure of new and currently existing systems. This development would then allow companies to freely capitalize on these infrastructures to offer better services and products.

Although the Protocol Sink Thesis still needs to prove itself in the long term, the financial industry is already adopting business models towards DeFi-based services, e.g, custody services for crypto assets. In addition, centralized crypto marketplaces such as Coinbase, Binance, and Opensea are engaging in competition with traditional brokers and exchanges. These exchanges allow users to participate in various revenue streams, e.g., staking, liquidity pooling, lending, or issuing and trading of NFTs (see Section 3).

The goal of this study is to shed light on the state-of-the-art of DeFi to comprehensively understand the technological foundations, the ecosystem as well as it's potentials and challenges. First, we present the technology-stack that powers DeFi by elaborating on its building blocks in Section 2, including blockchains, smart contracts, tokens, and digital wallets. In addition, we present the layers that compose DeFi. Next, we provide an overview of core DeFi application areas and use cases in Section 3. We then analyze the potentials of DeFi and evaluate related promises in Section 4. After that, we discuss current challenges in DeFi and approaches to possible solutions in Section 5. We conclude with a summary and an outlook in Section 6.

With our study, we hope to reach all those interested in DeFi, including those who want to use this work for initial research on the topic. We aim not only to demonstrate the potential of DeFi, but also to provide a dedicated assessment of key challenges that otherwise received little attention to date in research on DeFi. We believe that this encompassing overview provides a profound understanding on the emerging topic of DeFi, particularly, for investors, users, and decision-makers across all types of organizations and domains.

2 Foundations

2 Foundations

This section introduces the technological foundations of DeFi that are essential for understanding the concepts presented in this study. First, we delve into blockchains and smart contracts, which serve as DeFi's technical backbone. Second, we introduce further key components of DeFi considering its main objectives. Third, we present the DeFi-Stack that describes its different layers.

2.1 Blockchain Fundamentals

A blockchain is a type of distributed ledger technology (DLT). A DLT typically denotes a database in which the data storage is distributed across multiple entities. In a blockchain, the transactions are aggregated in batches, called blocks, which are cryptographically linked together, making it infeasible to alter transactions in retrospect. In addition, data on blockchain is stored transparently to allow for verification on its integrity. Therefore, blockchains are generally considered tamper-proof and transparent ledgers. Owing to their properties, blockchains can be implemented in domains beyond finance. In this regard, blockchains can add value, for example, in the energy (Djamali et al., 2021; Sedlmeir et al., 2021c), supply chain (Fridgen et al., 2019), public (Fridgen et al., 2018a; Roth et al., 2022), or sports sector (Schellinger et al., 2022a). Blockchains differ from other types of DLTs in their three main building blocks, i.e., a peer-to-peer (P2P) network, cryptographic primitives, and an incentive-based consensus-mechanism (Butijn et al., 2020). The combination of these building blocks enables the trustless execution and settlement of transactions in a decentralized setting, i.e., without the need for a central authority (Schlatt et al., 2016; Völter et al., 2021).

Peer-to-Peer Network

A blockchain represents a distributed and synchronized append-only database in which state-updates (in the form of blocks) are stored in a replicated way across all participants (Dinh et al., 2018). A block includes sequentially ordered transactions. For efficiency reasons, computers (***nodes***) that maintain their own, synchronized copy of the database also compute a ***world state***, i.e., a running aggregation of all previous state updates. By design, a blockchain is maintained on a multitude of nodes in a P2P configuration. Redundant data storage ensures the availability and integrity of the data, as well as protection against denial-of-service attacks. Proposed transactions that have not yet been confirmed by including them in a block are typically stored in a ***Mempool***. Based on the yet unconfirmed transactions in the Mempool, block-producers select transactions to be included in the next block (usually transactions with higher fees).

Cryptographic Linking

Blocks in a blockchain are cryptographically linked to one another using hash values of data. In addition to new transactions, a new block requires a hash-pointer to the preceding agreed-on block in the blockchain. These cryptographic links are required to achieve immutability of the blockchain: Any alteration in previous blocks would change the block's hash value and thus render the chain inconsistent ("tamper-evidence") (Samaniego et al., 2016). An ex-post modification that other nodes accept therefore requires the modification of all blocks subsequent to the manipulated one. Thus, consensus mechanisms are typically designed in a way that makes ex-post modifications increasingly difficult with the growing number of subsequent blocks (Nakamoto, 2008).

Consensus Mechanisms

The block creation process varies across different blockchains. Generally, the consensus mechanism relies on combining cryptographic techniques and economic or social incentive mechanisms to determine who may propose a new block. By committing processing-power (e.g., in proof of work (PoW)-based systems), locked capital (e.g., in proof of stake (PoS)-based systems) or reputation (e.g., in proof of authority (PoA)-based systems) to the network, block-producers or validators have a specific probability of being eligible to propose a new block (Wang et al., 2019). PoA represents a voting-based consensus mechanism, where a block is accepted once a (super-)majority of nodes approves it. A simple approach where each node has one vote, or the number of votes is connected to the corresponding entity's reputation, is only possible in ***permissioned*** blockchains where participating identities are restricted and known. Correspondingly, coupling a scarce resource like hardware and energy (PoW), capital (PoS), or storage in open, permissionless networks to voting weight is required to counter Sybil attacks. Sybil attacks involve an adversary who would aim to outvote honest participants by registering dummy accounts at low costs (Sedlmeir et al., 2020). Proposed blocks are then validated by the network using the specific consensus-mechanism and – if approved – appended to all replicas of the blockchain. Usually, the block-producer earns a reward for an accepted block in the form of newly created coins and transaction fees.

Heterogeneity of Blockchains

Besides these characteristics, blockchains are quite heterogeneous. They vary, for example, in their degree of openness (public vs. private) and eligibility to participate in the consensus mechanism (permissionless vs. permissioned). Public blockchains can be accessed, copied, and synchronized by anybody. In permissionless blockchains, any party can assume a role within the network and participate in consensus without needing the approval of one or several other entities of the network. In addition, while Bitcoin and other cryptocurrencies have been criticized for their high energy demand, many other blockchains – namely those that do not use a PoW-based consensus mechanism – do not have a problematic energy consumption (Sedlmeir et al., 2020). In particular, both PoS-based permissionless blockchains and permissioned blockchains that are usually using some voting-based consensus mechanism require several orders of magnitude less electricity than Bitcoin. In this regard, Bitcoin has often been criticized for its enormous energy requirements that rank among some medium-sized industrialized countries. Yet, less energy intense blockchains may even facilitate net energy savings by leveraging additional opportunities for digitizing cross-organizational processes (Rieger et al., 2022). The low energy consumption of PoS blockchains is one of the core reasons why some DeFi services decided to launch on PoS-based blockchains like Cosmos, Polkadot, or Tezos. Also, Ethereum is still undergoing a transition from PoW to PoS. In this view, regulators are actively discussing whether measures against PoW cryptocurrencies' high energy consumption should be taken (Gola & Sedlmeir, 2022).

DeFi applications typically rely on public and permissionless blockchains. However, there are applications built on permissioned blockchains since, among other reasons, these allow for improved performance. However, performance improvements come with a trade-off as more sophisticated and expensive hardware is required to participate in consensus.

2.2 Smart Contracts

A simple transaction in the blockchain ecosystem is the transfer of funds from one address to another. However, many more recent forms of blockchains have expanded upon that and allow for the execution of arbitrary deterministic program code. These executable programs on blockchains are referred to as ***smart contracts*** (Buterin, 2014; Szabo, 1996). In a smart contract, a code is deployed on the blockchain and thus available to audit and call (according to the code's rules) for every participant at any time (Buterin, 2014). On the Ethereum blockchain – arguably the most important DeFi blockchain at the moment – there are already many popular standards for the most common types of smart contracts. These standards are often specified in the form of Ethereum requests for comments (ERCs), for instance, the widespread ERC-20 for fungible and ERC-721 for non-fungible tokens. Through the asset layer, Ethereum also empowers programmers to implement decentralized applications (DApps), which leverage the Ethereum blockchain to record events. In addition, DApps track the ownership of digital assets that are relevant to the application and for which it should not depend on the availability or honesty of a trusted third party. In this light, smart contracts allow implementing DApps that represent complex applications or organizational structures, e.g., decentralized autonomous organizations (DAOs). The code is run in the creation phase of a new block. A user can then commit funds and input variables to a smart contract by sending a transaction. Upon inclusion of the transaction in a new block, the block creator runs the smart contract code using the given inputs and commits all resulting state updates – including transactions triggered subsequently according to the smart contract's logic – to the world state. Nodes that accept this new block also perform this computation and update their world state accordingly. Therefore, it is critical that smart contracts are ***deterministic***. Given the inputs of a transaction, changes in variables and the triggering of other methods must be identical for each node, otherwise the world states of the different nodes would diverge (Kannengiesser et al., 2021). Consequently, it is not feasible to simply query data from outside the blockchain, e.g., a website that provides data on weather or flight delays, in a smart contract operation. Thus, DApps require "oracles" which intermediate between the deterministic "blockchain environment" and the non-deterministic "outside" by making associated information available "onchain". An entity is then responsible for inserting outside-world data as payload in transactions that triggers a smart contract. As it is not possible to automatically and universally check for the veracity of this information, the blockchain relies on these agents to perform honestly and to report the correct information. This dilemma is often referred to as "the oracle problem" (Caldarelli & Ellul, 2021). Corresponding data is typically checked by a consortium of incentivized entities, cryptographic checks of provenance, or removing outliers and averaging the remaining data. Often, this involves combinations of incentives and punishments for inserting "good" or "bad" data.

2.3 Tokens, Transfers, and Wallets

Tokens play a central role in DeFi applications. However, the design and role of tokens can vary widely. Smart contracts can, for example, be used to create new tokens with a specific supply that follows a specific logic, and manage the corresponding ownership relations. Initially, smart contract-based tokens were often programmed and issued via initial coin offerings (ICOs), inspired by initial public offerings (IPOs) in TradFi. ICOs have been used by a variety of projects to fund early development, marketing, or to obtain initial liquidity (Arnold et al., 2019). Smart contracts can also be used to manage variables that represent control over the smart contract itself or other key parameters that it was built for. This is relevant, for instance, to offer the creator a degree of freedom to update or deactivate the smart contract. This built-in mechanism becomes handy in the case of implementation errors or extensions. However, it also bears risk, as the corresponding entity needs to be trusted not to abuse this power.

Depending on the smart contract's design, tokens can resemble units of a currency, equity, fractional ownership of an asset, voting rights, payments within an application, or an incentive in a network (Oliveira et al., 2018). The most common application of a token is that of a currency, where a fungible token represents a unit of account. Bitcoin's "BTC" and Ethereum's "ETH" are examples for such native protocol tokens, which are also central to uphold the corresponding blockchains' consensus mechanism by incentivizing the honest contribution of hashrate, capital or some other scarce resource, depending on the consensus mechanism. In this light, the native currency units serve as "fuel" for facilitating transactions in the form of fees that are needed to incentivize block producers' activities on the network. In a variety of blockchain protocols, validators are also rewarded with freshly minted native tokens once a new block has been accepted by the network. This is due to the fact that malicious behavior cannot be detected in a pseudonymous system since identities behind wallet addresses are not known, which makes it difficult to take legal action. Therefore, incentive mechanisms are implemented to reward honest behavior to ultimately maintain the integrity of the system (Bano et al., 2019).

Tokens in the context of the ERC-721 standard have been a relatively new development. They are NFTs, i.e., each token is unique and distinguishable from each other. Lately, NFTs have garnered attraction for being used as unique digital assets, e.g., digital artwork (Sunyaev et al., 2021; Whitaker & Kräussl, 2020). In addition, other widely-used standards have emerged that exhibit extended functionalities. In this light, the ERC-1155 standard allows to create a token in a smart contract that incorporates properties of both the ERC-20 and ERC-721 standard. The transfer of one of these tokens on the blockchain is one of the simplest forms of transactions: It usually involves saving the sender's and receiver's addresses as well as the amount of assets to be transferred (additionally, for NFTs the unique identifier is saved). By publishing the transaction in the next block, it is approved by the whole blockchain-network, and can be considered finalized. Tokens associated with an application can not only be used for the specific application, but can be freely transferred to many other DApps if they follow the standard templates (e.g., ERC 20 on Ethereum).

To access and manage these funds represented by tokens, associated with a unique address, participants need so-called wallets. Digital wallets generate and securely store cryptographic key pairs that need to be used to access tokens on a blockchain."Hot wallets" are essentially clients that communicate with blockchain nodes in the form of software applications running on a mobile phone or a computer. These kinds of wallets also display account balances and facilitate the interaction with blockchains. There are also specific tools to address security requirements. For instance, "cold wallets" store sensitive information and in particular private keys on air-gapped storage media, such as flash drives or QR codes, to prevent leakage to attackers.

2.4 Decentralized Finance

As shown, DeFi is characterized by an open, permissionless, and highly interoperable technology stack with strong integrity and availability guarantees. Proponents claim that it promotes financial inclusion, efficiency gains, and flexibility (Schär, 2021). DeFi aims at replicating financial services and products. Further, it creates entirely new DApps in an open and transparent way built on blockchains and smart contracts. Owing to the degree of decentralization of the underlying blockchains, DeFi does not rely on a single intermediary or centralized institution, such as banks, brokers, or exchanges (Feulner et al., 2022a). Instead, agreements are enforced by code and consensus, which allows transactions to be executed in a secure, predictable, and verifiable way, with legitimate state changes persisted on a public, tamper-proof ledger. Noteworthy, this does not mean that every DeFi application is fully decentralized (see Section 3). Yet, the transparent record of transactions on public ledgers and publicly available code enable an immutable and highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services (Schär, 2021).

According to Schär (2021), the DeFi ecosystem can be subdivided into five different layers; Figure 2 illustrates this stack exemplary for Ethereum:

- ***Settlement Layer***: The settlement layer is represented by a blockchain-based distributed database that manages basic accounting operations, maintains access to funds, and executes transactions. A consensus mechanism and basic cryptography like digital signatures and cryptographic hashing algorithms ensure security and integrity guarantees in a decentralized manner.

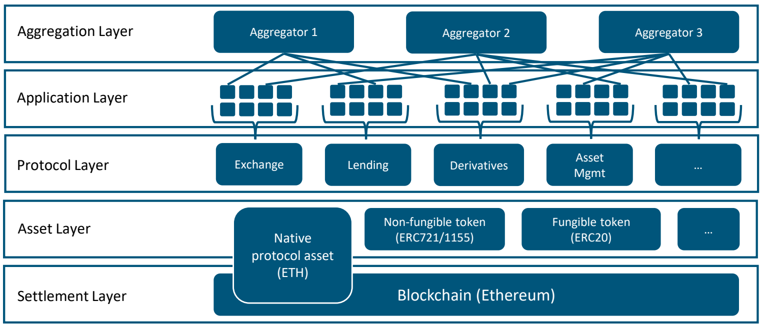
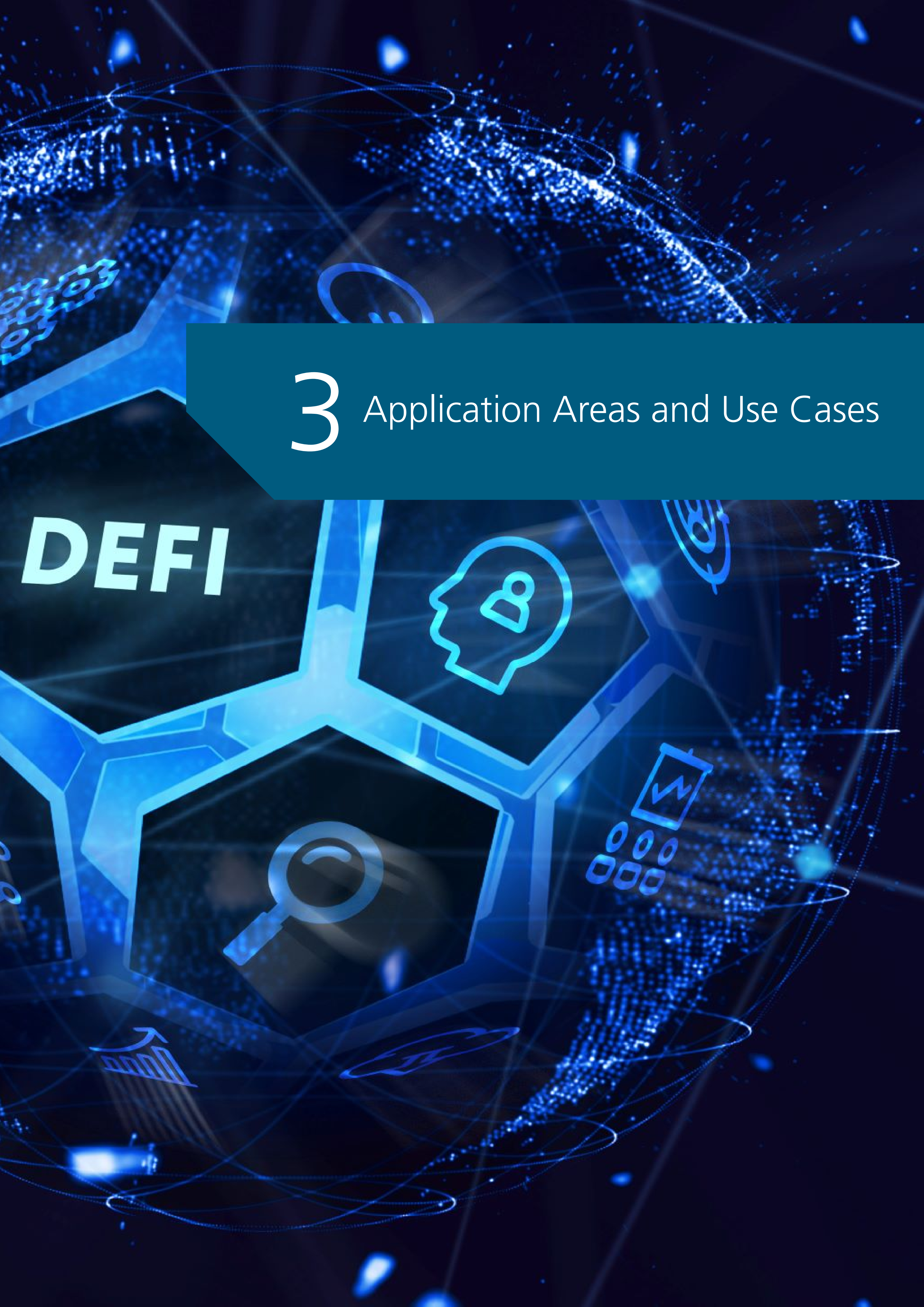


Figure 2: The DeFi-Stack on Ethereum (based on Schär (2021)).

- *Asset Layer*: Different digital assets can be created and traded on top of the settlement layer. Beyond the simple use of such an asset as a store of value or medium of exchange, DeFi also allows users to act as service providers. Users can supply assets to DeFi applications or hold tokens that represent a share of a project, granting governance rights.
- *Protocol Layer*: The protocol layer includes smart contracts that try to provide a standardized solution or service, e.g., a general way to allow for the exchange of different cryptocurrencies. Protocols represent ubiquitous services (Sedlmeir et al., 2022) that can be as sophisticated as DAOs that represent complex organizational structures. They enable the execution of general, deterministic code for a variety of applications, such as exchanges, lending, or derivatives.
- *Application Layer*: A combination of smart contracts as backend and a web-based frontend results in a DApp. These applications make DeFi services accessible to a broader user base through user interfaces and may integrate several of these highly composable protocols to allow more complete services. This could, for instance, include a service that integrates several currency protocols and an exchange protocol into a single decentralized or centralized exchange (Tabora, 2021).
- *Aggregation Layer*: The aggregation layer enables aggregator applications by integrating services that can be technically independent of one another. However, these DApps provide more utility if made accessible combined by a single aggregator. For instance, this could comprise several insurance services that join one larger DeFi-based insurance platform.

It becomes apparent that these layers build on each other and that the different DeFi layers are not strictly separated but interwoven. Owing to the interoperability and composability of smart contracts, DeFi often uses the notion of “money Legos” (Katona, 2021; Schär, 2021). In a more narrow view, the term DeFi primarily refers to upper layers, i.e., the protocol, application, and aggregation layers of the model proposed by Schär (2021). However, the asset and settlement layer act as a technical infrastructure and common foundation. Thus, it is an essential part in the DeFi-Stack.



3 Application Areas and Use Cases

3 Application Areas and Use Cases

Bitcoin was the first system that enabled the transfer of value in a decentralized P2P network, therefore innovating electronic payment systems beyond traditional, centralized architectures. Ethereum then extended the capabilities of blockchain-based systems far beyond simple payments. In particular, smart contracts facilitate a broader range of applications that offer a high degree of customizability and programmability.

A considerable portion of these applications fit into the category of DeFi, which focuses on the replication of financial services. Against this background, smart contracts have enabled the community to develop innovative and complex DApps, DAOs, and digital tokens. DeFi hereby comprises a wide range of different application areas that have considerably grown in value locked, most notably in 2021. Figure 3 summarizes the DeFi applications presented in this section. The two main sectors identified are financial services or markets and gaming or gambling. As explained in section 2, the DeFi ecosystem is closely interconnected and for most protocols there is neither a clear-cut between the two main categories nor between the subcategories. In fact, there are many protocols that cover multiple subcategories. Also, a multitude of gaming or gambling protocols rely on financial building blocks. Conversely, many core DeFi services (i.e., finance-related DApps) incorporate gamification elements to increase user adoption. In the following, we will present these relevant application areas and provide illustrative examples for a better understanding of DeFi projects.

3.1 Stablecoins

Owing to substantial financial speculation, market manipulations from large token holders (i.e., “whales“), and relatively low liquidity, cryptocurrencies typically face severe price fluctuations, impairing their ability to be a medium of exchange and reducing liquidity in cryptocurrency markets (Griffin & Shams, 2020). A medium of exchange requires a certain price stability to a broad range of products, which is a complex task of money supply and demand management and is usually performed by a central bank. In this light, stablecoins have emerged, aiming to provide a stable exchange rate to a pegged value, e.g., fiat currencies, commodities, or gold. Thus, stablecoins constitute a digital asset whose price is either pegged to the value of an underlying reserve asset or maintained by algorithms. Yet, the main goal of stablecoins resides in providing a cryptocurrency with as little volatility as possible (relative to established currencies like the USD) to fulfill the need for a stable medium of exchange in economy. In addition, less volatile crypto assets are important for financial products and services in the DeFi ecosystem. Thus, stablecoins represent a crucial part of DeFi and are expected to boost widespread adoption of DeFi applications (Catalini et al., 2021). Figure 4 illustrates the historic market capitalization of the top five stablecoins.

In general, several types of stablecoins exist that depend on the type of the underlying reserve asset – the collateral (Klages-Mundt et al., 2020). Foremost, there are stablecoins that are pegged to one or more commodities, fiat currencies, or other “stable” real-world assets. Just like within the origins of fiat currencies, the value of coins are, thus, based on the promise of an issuing party that the amount of circulating stablecoins is backed by the amount of underlying assets, making them redeemable for the underlying asset at any time. Fiat-backed stablecoins, for example, peg each coin directly to a certain amount of fiat currency. This peg is realized off-chain and requires a financial institution that serves as a custodian for the currency used to back the stablecoin. In addition, off-chain collateralized stablecoins demand trust in centralized custodians in terms of backing the asset or fiat currency for the stability of the coin. Accordingly, these stablecoins are often not considered as truly decentralized crypto assets and are vulnerable to depreciation if the backing cannot be verified.

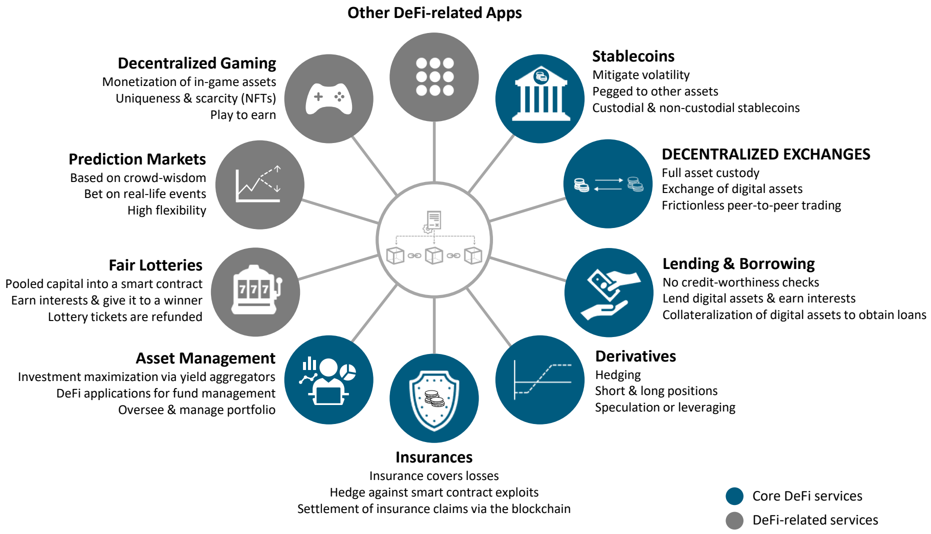

Other DeFi-related Apps
Stablecoins
Mitigate volatility
Pegged to other assets
Custodial & non-custodial stablecoins
DECENTRALIZED EXCHANGES
Full asset custody
Exchange of digital assets
Frictionless peer-to-peer trading
Lending & Borrowing
No credit-worthiness checks
Lend digital assets & earn interests
Collateralization of digital assets to obtain loans
Derivatives
Hedging
Short & long positions
Speculation or leveraging
Insurances
Insurance covers losses
Hedge against smart contract exploits
Settlement of insurance claims via the blockchain
Asset Management
Investment maximization via yield aggregators
DeFi applications for fund management
Oversee & manage portfolio
Fair Lotteries
Pooled capital into a smart contract
Earn interests & give it to a winner
Lottery tickets are refunded
Prediction Markets
Based on crowd-wisdom
Bet on real-life events
High flexibility
Decentralized Gaming
Monetization of in-game assets
Uniqueness & scarcity (NFTs)
Play to earn
● Core DeFi services
● DeFi-related services

Figure 3: Summary of core DeFi and DeFi-related service categories.

The second category includes seigniorage stablecoins whose stability is based on an algorithm that maintains the coin price close to an intended peg (e.g., USD 1). This is achieved by automatically expanding and contracting the coin supply – similar to how central banks mint or burn money (Sams, 2014). Unlike other categories, Seigniorage stablecoins are therefore the only category which is not actually backed by any underlying asset. The missing collateralization poses several questions and hurdles, e.g,. if the coin will be stable in value when there are high (alternating) price fluctuations. Depending on the definition, it is often questioned if they can be considered as stablecoins at all (Crown, 2018). Noteworthy, the algorithmic stablecoin UST (Terra USD) of the LUNA ecosystem was the fourth largest stablecoin in the DeFi ecosystem until April 12, 2022. After massive selloffs in the wake of a general DeFi downturn (see Figure 1), UST lost its peg to the USD and its market capitalization fell from approx. USD 19 billion to USD 70 million (Barthere et al., 2022). Consequently, this development lead to downturns in the whole cryptocurrency market that also caused financial turmoil of centralized institutions, e.g., in the case of Celsius (Blockworks, 2022b) or 3 Arrows Capital (3AC) (Blockworks, 2022a).

Finally, the third type of stablecoins is issued using other cryptocurrencies as underlying asset. Conceptually, this is similar to fiat-backed stablecoins, but with the important distinction that the backing happens completely on-chain using smart contracts. This means that stablecoins are minted once a user locks a cryptocurrency as collateral into a particular smart contract. Since the value of the underlying cryptocurrency is exposed to price fluctuations, these stablecoins need to be over-collateralized. The smart contract then grants the user access to a certain amount of stablecoins, depending on the mandatory (over-)collateralization rate and the value of the (crypto) reserve asset.

A prominent example for a crypto-backed stablecoin is DAI of the MakerDAO protocol (Brennecke et al., 2022). We illustrate how these stablecoins work by introducing an example where Alice wants to get the equivalent of USD 100 in DAI stablecoins. As DAI is an Ethereum-based token, the collateralization occurs completely on-chain. This means that Alice sends Ether as collateral to a particularly designed smart contract governed by the MakerDAO protocol. To ensure price stability, the DAI rate is pegged to the USD and has to be secured with at least 150 % of the collateral (Ether).

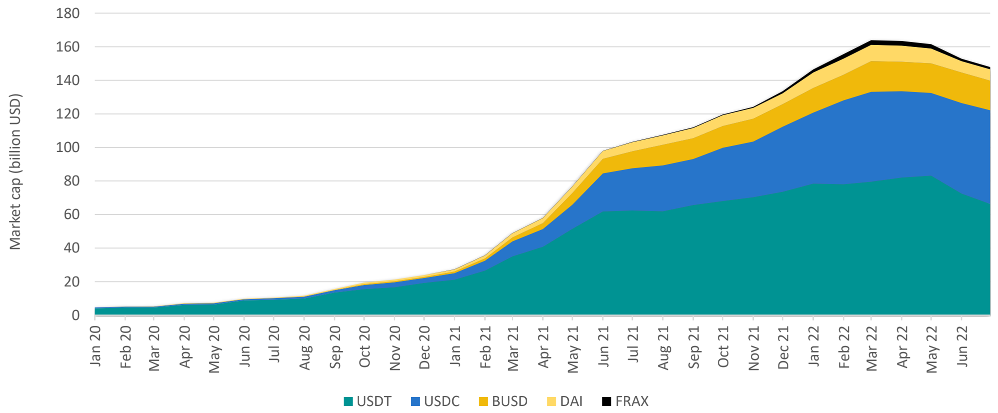


Figure 4: Market capitalization of the most relevant stablecoins (Data retrieved from Glassnode (2022)).

As Blockchains cannot access data outside their own state, "oracles" are necessary to provide pricing information. Within the collateralization for on-chain assets, decentralized exchange rates, and within auctions, order books or automated market making applications can be used to derive price information. For Alice, this means that she needs to send Ether as a collateral within the smart contract. In our example, the provided Ether have to be worth at least USD 150 based on the current exchange price (given by the oracles). The contract then allows Alice to withdraw DAI worth USD 100. As the DAI is pegged to the USD, the value of the collateral (i.e., Ether) locked in the smart contract will be continuously checked and if its value falls below the mandatory liquidation rate of 150 %, an automated auction of the reserve asset is enforced. Alice is obliged to pay a penalty for the auction, motivating her to secure her coins with a collateral deposition well above the 150 % ratio. In markets with high volatility and network congestion, the liquidation process can carry significant risks for users. Nonetheless, this mechanism enables an entirely decentralized and automated self-stabilizing system.

In general, stablecoins can be used across the whole DeFi ecosystem as long as they are compatible to the underlying blockchain infrastructure of the coin. For example, DAI is native on the Ethereum blockchain. Possible use-cases for stablecoins include exchanging them to another currency (crypto or fiat), using them to de-risk without the need of withdrawing the money from the DeFi ecosystem, offering the possibility of keeping a long-position on the reserve asset and borrowing against it to still having liquid capital (due to the collateralized debt position), buying more units of the reserve asset at a decentralized exchange in the DeFi ecosystem, leveraging beneficiary exchange prices, and earning interest using lending and borrowing platforms. Overall, within all these areas of application, users are able to make use of their investments without having to sell the underlying collateral. Finally, stablecoins can also be used for remittance or salary payments to avoid high intermediation costs or to mitigate volatility and currency risks of local currencies.

Another type of cryptocurrency that aims to provide a low-volatility currency that is pegged to a certain basket of assets, are decentralized reserve currencies. They can be viewed as a special form of crypto-backed stablecoins, but instead of keeping a peg to a fiat currency like the USD, they are pegged to a basket of assets, mainly composed of different cryptocurrencies. The performance of them therefor can be compared to an exchange tradable fund (ETF), which volatility mainly depends on the volatility of the individual assets, their correlation and its diversification. The main reason for their emergence was the growing importance of stablecoins in the ecosystem and the reintroduction of centralized institutions behind them. Decentralized reserve currencies therefore try to take the autonomy of DeFi one step further to be independent of centralized institutions holding fiat reserves and also to not be limited to low volatility assets that are pegged to fiat currencies and other commodities. The first protocol to implement this mechanism was OlympusDAO which reached a value of controlled assets of up to USD 800 million. [1] Inspired by the success of Olympus, many other decentralized reserve currencies emerged with various asset compositions and different success regarding their growth and price stability.

3.2 Decentralized Exchanges

A decentralized exchange (DEX) provides the advantage of not having to rely on a single, non-transparent, trusted entity as the market maker who might work in their own favor, get hacked, or outright disappear with entrusted funds. It also avoids problems of re-centralization. Traditional exchanges rely on order books. A centralized party stores demand- and supply-orders and matches them by pairing a buy with an opposing sell decision for an equal amount and price. In terms of trading volume and total value locked (TVL), the value committed to certain smart contracts – decentralized order book exchanges – play no significant role in the DEX space yet: Owing to the expensive storage space and computation on a blockchain, and considering that setting and matching an order results in separate transactions, the fees of this approach would be very high. Nevertheless, technologies like zero-knowledge proofs (ZKPs) or layer 2 (L2) solutions used in new applications on established or entirely new blockchains (see Section 5) could make order-book DEXes a more viable option for DeFi in the future. Currently, Polkadex and Serum are first growing players running on-chain order books. This approach is advantageous – in contrast to the automated market makers (AMMs) which we discuss below – as orders backed by liquidity can be pooled without the need for external liquidity providers.

To date, most popular DEXes operate based on an AMM algorithm. Hereby, a liquidity pool holds both assets of the trading pair and acts as counterparty to trades. An algorithm determines the exact amount and price at which an order is executed that is based on the ratio of the assets in the liquidity pool. When trading against this liquidity pool, that is supplying only one asset and receiving the other asset, the pool ratio shifts and the price moves. The size of the price movement depends on the ratio of trade size to liquidity pool size and the pool's algorithm. A simple example is the curve-function $R_x \cdot R_y = m$ used by the ***constant function market maker*** Uniswap: For each additional increment of currency x added to the Reserve R_x, the marginal amount of units of currency y bought from the Reserve R_y becomes slightly less so that the price increases with the size of the buy order (see Figure 5). The special curve-function ensures automation and allows for efficient and fair collaborative pricing without the need for a centralized order book. Further, liquidity is created by dedicated "liquidity providers", who provide both assets of the trading pair in the current ratio to the liquidity pool. While on centralized exchanges (CEXes), market makers are often a responsible for keeping even exchange rates on different exchanges, DEXes need arbitrageurs that use price discrepancies in order to reach price equilibrium. Since arbitrageurs profit from the price discrepancies that they balance out, the liquidity providers are exposed to "impermanent loss" due to price movements caused by arbitrage trades: After they have provided their liquidity, their liquidity position can become worth less than it would have been if they just had held the assets they conveyed when the relative value of the two assets changes. In order to compensate for impermanent loss, and to incentivize liquidity provisioning, liquidity providers receive a share of the trading fees that

[1] See Market value of treasury assets in OlympusDAO.

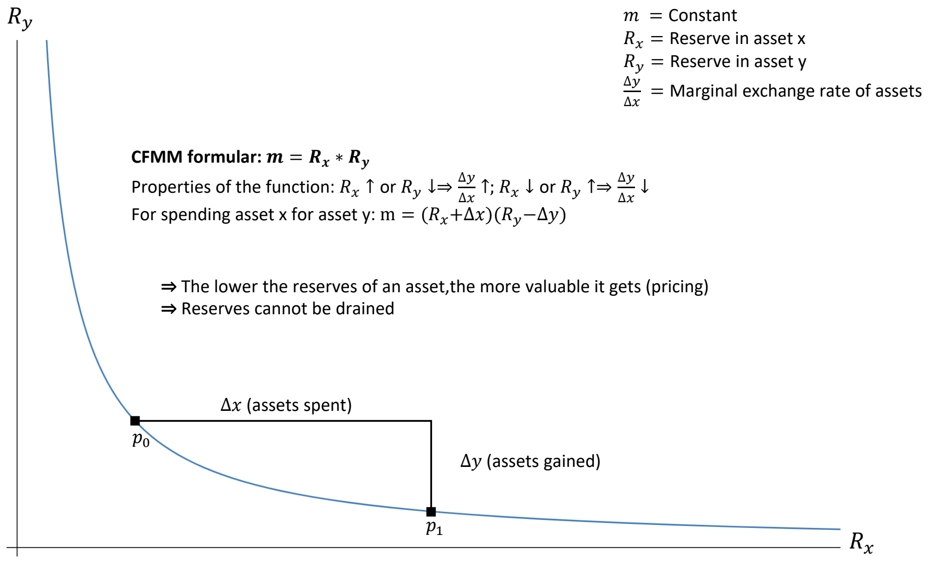

R_y
m = Constant
R_x = Reserve in asset x
R_y = Reserve in asset y
$\frac{\Delta y}{\Delta x}$ = Marginal exchange rate of assets
CFMM formular: $\boldsymbol{m = R_x * R_y}$
Properties of the function: $R_x \uparrow$ or $R_y \downarrow \Rightarrow \frac{\Delta y}{\Delta x} \uparrow$; $R_x \downarrow$ or $R_y \uparrow \Rightarrow \frac{\Delta y}{\Delta x} \downarrow$
For spending asset x for asset y: $\mathrm{m} = (R_x + \Delta x)(R_y - \Delta y)$
⇒ The lower the reserves of an asset,the more valuable it gets (pricing)
⇒ Reserves cannot be drained
Δx (assets spent)
p_0
Δy (assets gained)
p_1
R_x

Figure 5: Constant Function Market Maker (based on Bartoletti et al. (2021) and Xu et al. (2021)).

are generated from the pool. Most AMMs further incentivize liquidity suppliers by distributing their own protocol token to liquidity providers. We limited our illustration of AMMs to a simple archetype which shows how an AMM algorithm can be constructed. Uniswap, Curve, and Bancor are the most notable DEXes at the moment, yet, they each use different interpretations of AMM-algorithms.

3.3 Lending and Borrowing

Similar to how DeFi establishes spot exchanges by use of AMMs, DeFi also enables the seamless P2P lending and borrowing of crypto assets. However, AMMs for lending and borrowing do not price assets against each other like on DEXes but determine the interest rate on a given asset, based on its utilization rate (total loans divided by total deposits of the asset) (AAVE, 2020; Compound, 2020). The interest rate function can be either linear, non-linear (e.g., dYdX), or kinked (e.g., Compound and AAVE), determining at which rate the interest rate increases or decreases, which represent the main incentive for lending and borrowing. Lenders lock their crypto assets in a smart contract and earn variable interest on locked currencies. These funds can then be borrowed at fixed or variable interest rates. The assets borrowed need to be backed by a collateral deposit consisting of another asset to ensure liquidity in the absence of credit-worthiness due to pseudonimity.

Over-collateralization defeats the financing purpose of a loan per se, however, lending and borrowing protocols are important and mainly used for providing further financial utility such as decentralized margin trading for borrowers (e.g, short sells and leveraged longs) and easy, relatively safe, and trustworthy investment of crypto assets for lenders (Gudgeon et al., 2020b). Additionally, these protocols, in conjunction with stablecoins, play a substantial role in providing the DeFi ecosystem with liquidity. At the time of writing, four out of the ten biggest Ethereum applications in terms of TVL are such lending protocols. As of June 2022, Aave is currently the biggest lending application, with roughly USD 5 billion locked (DeFiLlama, 2022).

3.4 Derivatives

A financial derivative is a contract which derives its value from the performance of an underlying asset. They are commonly used in the financial world to decrease risk (by hedging) or to purposefully increase exposure to an asset without having to buy the asset itself in hopes of benefiting (by leveraging) from the increased risk.

Derivative applications for margin trading are implemented similar to the lending and borrowing protocols, with the main difference that additional derivative-specific smart contracts automate and facilitate the orders for margin trades (e.g., leveraged longs and short sells). In options trading, a buyer of a derivative pays a premium to the issuer executed by a smart contract. In addition, the smart contract controls the underlying asset. As a last step, the smart contract issues a new token that represents the option (Juliano, 2018). This token can then be sold to others or used to exercise the option, similar to options in TradFi. These derivatives can function without time and price feed oracles by using the Unix time stamp of blocks and decentralized pricing mechanisms of AMMs. However, there also exists the possibility of a smart contract that tokenizes, i.e., converts real-world objects into a blockchain-based form, these financial derivatives using oracle price feeds (e.g., Synthetix). This mechanism enables the creation of non-crypto assets in DeFi.

Lately, a growing number of DeFi derivatives on “real-world” assets can be observed. Price data on real-world assets is usually provided through oracles, so that any asset for which an oracle exists can be described by a derivative, while the value of common crypto assets can also be derived from lookups on DEXes (Synthetix, 2022). This allows users to hedge or leverage open positions not only on crypto assets, but increasingly on real-world assets in a far easier way than TradFi would allow. For example, dYdX offers derivatives on cryptocurrencies with up to 25x leverage, while Synthetix, provides derivatives on crypto assets and fiat currencies, commodities, stocks, and indices. Protocols like Hegic and Dopex supply more traditional derivatives like call or put options, as well as future contracts.

3.5 Insurances

Given the novelty of DeFi applications, the risk of smart-contract hacks and bugs embedded in the code is extremely high, creating a need for insurance coverage to protect against such risks. These risks can have severe consequences on the integrity and adoption of DeFi applications, e.g., in the case of the DAO (Dhillon et al., 2017) or Poly Network hack (Gagliardoni, 2021). Since smart contracts are publicly available code snippets, anyone can search for flaws and exploit them. Against this background, users can cover losses resulting from bugs or attacks in smart contracts by purchasing dedicated insurance products (Guggenberger et al., 2021a). For instance, Nexus Mutual and Opium Finance provide insurances that cover smart contract risks. Other insurance applications in the DeFi space are gaining traction as well. Through the use of oracles, virtually any real-life risk can be insured using DeFi-based insurances. Arbol, for example, uses oracles for weather-data to insure farmers against the loss of crop yield, should certain weather parameters be met. Another example, Etherisc, automatically compensates customers of delayed flights. In such cases, the settlement of insurance claims can be handled digitally and virtually instantaneously, in contrast to most real-world insurance procedures. On the other hand, implementing a purely smart-contract based insurances in DeFi is arguably challenging, as, for instance, a hack is difficult to prove purely based on transactions that the hack involved. To address this issue, for example, a DeFi-based insurance platform could establish a competent contingency committee composed of insurance experts and advised by independent IT auditors who assess the claims. Based on the vote, the insurance claim is either settled or declined (Guggenberger et al., 2021a). While this procedure can solve the problem of proving the occurrence of an insured event, it reintroduces trusted intermediaries. Therefore, it remains unclear to which extent the dependence on trusted intermediaries inhibits the utility of insurance products in DeFi.

3.6 Asset Management

Crypto assets offer an opportunity for portfolio diversification and, thus, mitigation of risk (Schellinger, 2020). Additionally, beyond pure crypto investments, DeFi enables automated digital asset management. In DeFi, funds can be locked in smart contracts controlled by DApps that invest and manage crypto tokens. Asset management tools come in a plethora of different innovative approaches and designs. A widespread use case is the automated investment in existing DeFi protocols, where the weighting of different positions is determined by an algorithm or personal preferences. Asset management in DeFi is largely defined by yield farming protocols, such as Yearn.finance and Pickle.finance (Guazzo, 2020). These portfolio management applications offer "vaults" where users can deposit their assets. Each vault comprises different investment strategies for the asset, which are developed, optimized, and tested off-chain by strategists (Yearn Finance, 2022b). Usually these strategies encompass an initial investment of the original assets into a liquidity pool of a DEX and then re-invest the tokens awarded for providing liquidity to another DApp and so on. Hence, yield farming spans a variety of existing applications of the DeFi ecosystem. Based on the changing yield values of these strategies, the vault then routes the funds through the strategy which currently allows for the highest return. When interest rates change on various DeFi platforms, the vault automatically reallocates its assets to a better strategy, if one is available (Yearn Finance, 2022a).

Through smart contracts or tokenization, establishing social investing where one investor manages the digital assets becomes convenient. Moreover, others can follow or stake these investments – often for a fee that can amount up to 20 % of the earnings – by simply engaging with a provided smart contract. DeFi also offers a lot of potential for automation, as transactions are only engagements of smart contracts they can be triggered one after another within one main call. This can be used to take out a "flashloan" ("flash" due to their short lifespan) to benefit from arbitrage. As such, flashloans initiate a succession of rapid transactions with the borrowed money and pay back the loan within a single call. One tool to facilitate such atomic transactions is Furucombo.app, where users can easily create their own trading bot through a drag-and-drop interface.

There are also applications that address the problem of conditional orders (i.e., stop-loss orders) within DeFi which are usually individual transactions on most DeFi protocols and, thus, cause transaction fees for each change of an order. Services can manage these conditional orders on their own layer and only execute them on the main chain once the condition is met. The landscape of DeFi protocols is highly fragmented on a technical level over several blockchains and on an interaction level over a variety of websites and DApps. Standardization is important to overcome these challenges arising from a common digital infrastructure with a multitude of incompatible interfaces. Prevalent asset management tools try to overcome this lack of standardization by aggregating important investment, liquidity, lending, and NFT protocols in their services and allow users to interact through a unified interface. Zerion.io for example claims to be the most extensive aggregation of DeFi-protocols across chains and platforms. However, the high volatility and dynamics in DeFi ecosystems require asset management DApps to be highly agile (Dedezade et al., 2020; DKCrypto, 2021).

Furthermore, the management of crypto assets includes taking advantage of "airdrops". Airdrops describe the free distribution of tokens to early users and investors of blockchain projects (CoinBundle, 2018). The rationale behind airdrops are primarily marketing purposes, as giveaways of valuable funds generate awareness for the project, while rewarding users and keeping them invested (Gunther, 2021; Solanews, 2021).

3.7 DeFi-related Applications

In addition, other non-core financial applications have emerged and are increasingly growing. These applications have a non-financial business logic, yet, relying on DeFi services and products, e.g., fair lotteries, prediction markets, and decentralized gaming.

- ***Fair Lotteries:*** Regulators often restrict the kind of bets that one may place or take significant fees for lotteries. DeFi applications try to mitigate these restrictions by constructing cheap, accessible, and mostly fair lotteries. The most notable lottery is provided by Pooltogether.com, where locked assets are invested, and locked coins equal one ticket for a weekly lottery of the return on investment. Lotto.finance has a more traditional approach, where tickets in the form of tokens are bought, and each token holder is automatically debited one token per lottery drawing, which are held twice a week.
- ***Prediction Markets:*** Prediction markets are created to predict, or rather bet on, the outcome of real-life events. Virtually any real-life event can be priced in these markets, e.g., applications ranging from predicting future prices of cryptocurrencies (e.g., omen.eth, plotx.io), sports-betting (e.g., augur.net) or on real-life events, for example betting on Polymarket.com if the rate of inflation will reach a certain threshold. Through crowd wisdom, a price is found for both options, representing the sentiment of all betters (Augur, 2018).
- ***Decentralized gaming:*** Decentralized gaming describes computer games that are built on and operated by decentralized technologies, e.g., blockchain. Especially regarding the possibility of monetizing in-game assets, DeFi and decentralized gaming offer a new paradigm for players often referred to as "play to earn" (e.g., Ubisoft Quartz). Therefore, decentralized gaming can provide many advantages. For instance, players can trade in-game assets between gaming applications or exchange them for crypto or fiat currency. In addition, users can borrow and lend in-game assets to other players. Lastly, users can benefit from earning passive income on their in-game assets, e.g., by staking them in liquidity pools (Krion, 2021). While these opportunities are specifically useful to reduce the dependence on the company that creates the game, one needs to take into account that owing to the capacity bottlenecks of blockchains, games usually do not happen entirely on-chain and therefore continue to build significantly on proprietary, closed-source software. Consequently, it is unclear to which extent computer game manufacturers will implement the interaction with blockchain-based gaming assets in a way that makes them useful also, for instance, across different versions of the same game, let alone across different games built by different manufacturers.

4 Potentials

4 Potentials

DeFi is still at an early stage of development, yet it offers a wide range of applications, which we have highlighted in the previous section. Together, these aspects suggest considerable economic potential, which we will discuss in the following section. In addition, we address the impact that DeFi could have on various aspects of society and present other specific business areas that could be affected by DeFi.

4.1 Financial Inclusion and Independence

The main goal of a financial system is to improve capital efficiency, which is achieved by intermediation between suppliers and demanders of funds on different financial markets using respective financial instruments (Cadete de Matos et al., 2021). TradFi hereby mainly operates in a hub-and-spoke structure in order to be efficient, for instance, by pooling financial activity and cutting costs (Lipton & Hardjono, 2021). However, this makes TradFi an inherently centralized and opaque financial ecosystem, where assets are often held in custody by third parties and access is limited due to geographic constraints (Derviz et al., 2021; Zetzsche et al., 2020).

Although online banking has made financial services more accessible, approximately 1.4 billion people worldwide are still considered "underbanked", especially in developing countries (The World Bank, 2018, 2021). Consequently, financial inclusion remains a broad socioeconomic challenge to be resolved even today. The reasons for this situation are manifold, e.g., the lack of local branches owing to overhead costs or efforts to comply with regulations, general distrust in banks and custodians, or failing minimum fund requirements (The World Bank, 2021).

As opposed to TradFi, DeFi represents a decentralized and transparent financial ecosystem that facilitates access to financial services. Instead of relying on a branch office to obtain financial services or obtaining permissions to operate in such systems, DeFi applications require an internet connection and a device to interact with the system (Derviz et al., 2021). By replacing intermediaries with smart contracts (e.g., AMMs), DeFi enables trustless and decentralized (P2P) financial markets using blockchains as a source of trusted settlement (Schär, 2021). Since smart contracts act as ubiquitous, fully automated service providers, DeFi provides access to financial services at any time. DeFi thereby provides permissionless financial services detached from geographical and formal restrictions, enhancing total self-custody (Qin et al., 2021a). In addition, reducing intermediaries to a few protocols has the potential to reduce additional fees. In this way, DeFi could become more accessible and beneficial to less affluent people around the world (Schär, 2021). Hence, proponents argue that DeFi could offer a remedy to the un(der)banked people worldwide, thereby boosting financial inclusion and independence (Y. Chen & Bellavitis, 2020; Katona, 2021; MakerDAO, 2020; Qin et al., 2021a). For instance, DeFi has seen a growing increase in usage across developing countries such as Vietnam, India, and Pakistan and many other countries in South America, where it is often perceived as a means to extend financial inclusion, open up new job opportunities, or access more stable (foreign) currencies (Chainalysis, 2021; Tornaghi, 2022).

4.2 Innovative Asset Classes and Funding Opportunities

As mentioned in Section 3, DeFi requires digital currencies, i.e. tokens, which are crucial for storing value and payments in this ecosystem. In addition to cryptocurrencies and in particular stablecoins, DeFi asset classes include governance and security tokens that are similar to traditional stocks (Oliveira et al., 2018). Organizations offering these tokens can range from traditional companies to DAOs. While DAOs incorporate these tokens by means of smart contracts, conventional businesses need to tokenize their shares. In general, these tokens grant ownership and voting rights in this entity, including payouts such as "dividends" (Barbereau et al., 2022c).

Furthermore, there are tokens that have a specific use in DeFi, such as paying for services provided by a DApp. Both asset classes, tokens that represent ownership and voting right, and tokens that provide access to services, can be used to fund projects in DeFi and are often initially launched and distributed via ICOs and airdrops. However, the main venues for distributing these tokens are traditional and decentralized exchanges. In this context, initial exchange offerings (IEOs) are token launches on a regular TradFi exchange, while initial decentralized exchange offerings (IDOs) are the counterpart launched on DEXes (Coinmarketcap, 2022b). A project that wants its token to be listed on a traditional exchange typically needs to meet formal requirements and quality standards in order to get listed (Anson, 2021). In contrast, IDOs provide the opportunity for everyone to list and launch their tokens – which, of course, also bears increased risk. DEXes provide a market with low entry barriers and a higher degree of (yet rarely perfect) anonymity, since users do not need to go through sophisticated know your customer (KYC) processes. In contrast CEXes offer a broader user base to the project as well as a certain level of authority and security with regard to fraudulent projects (Anson, 2021; Aspris et al., 2021). Many projects that end up getting listed on CEXes start with a DEX listing and proceed to attempt the cross-listing on a CEX later on in the project's life cycle. DEXes hence are suitable for financing early stage projects while CEXes – in line with their integration in regulatory domains – fulfil a gatekeeper role by certifying the quality and credibility of finished projects. Thus, they ensure further financing possibilities for developed projects by opening them to more risk-averse investors (Aspris et al., 2021). In the past, CEXes offered high amounts of liquidity, however, at present, the largest share of liquidity and trading volume for many projects and their respective tokens can be found on DEXes. This can lead to the token only being listed on a DEX, resulting in many, especially DeFi-native projects.

Analogously to what we described in Subsection 4.1, DeFi enables the process of financing projects to be less costly for anyone involved. Lower costs can be achieved by cutting the middlemen and reducing bureaucracy regarding compliance (Arnold et al., 2019). Moreover, given different types of assets, for example, native tokens, fungible tokens, and NFTs, DeFi funding tools are highly customizable to individual use cases and can range from providing utility and ownership such as shares to a token for crowdfunding (Bachmann et al., 2019; Fridgen et al., 2018b). In addition, smart contracts can be used to separate different utilities and authorizations that a token provides to its owner. For instance, governance tokens' trading rights could be traded separately from the token as a pure means of speculation or investment (Buterin, 2021). Fungible tokens are mostly used for purely financial (core DeFi) purposes, while non-fungible and semi-fungible tokens [2] are more widespread in further use cases. These tokens do not need to be associated with finance but can also be used in combination with hobbies. For example, collecting NFT trading cards (e.g., CryptoKitties and Bored Apes), enabling fan interaction in sports (e.g., NBA Top Shot NFTs and Socios Fan Tokens) or even representing forms of ownership.

Another interesting opportunity to use DeFi assets for financing purposes comprises "liquidity mining". Liquidity mining is tightly connected to trading on DEXes. As we described in Section 3, opposed to TradFi exchanges, DEXes have no central intermediary that acts as market maker by maintaining an order book. Instead, they have to rely on liquidity providers that provide liquidity for certain asset pairs to DEX liquidity pools, which in turn then act as market makers. Liquidity providers enable AMM DEXes by providing liquidity to the respective liquidity pool (asset pairs) in return for a share of the total trading fees that the DEX earns on every swap. The share can be determined, for

[2] Semi-fungible tokens can change their fungibility status between non-fungible and fungible during their life cycle.

instance, by utility or governance tokens received for supplying liquidity. This process is also known as liquidity mining and a profitable way to put capital to efficient use in DeFi. Supplying funds to lending pools works analogously by supplying an asset to its respective pool, where it gets loaned out for a small fee that then gets distributed amongst the suppliers of the lending protocol as means of a reward. Many lending protocols also incentivize lending and borrowing by subsidizing the rates with an additional distribution of the protocol token. In contrast to liquidity providers for AMMs, liquidity providers for lending protocols do not face impermanent loss.

Tokens in DeFi-based DApps can not only be used for this specific application, but can be freely transferred to many other DApps if they follow one of the common standards (e.g., ERC 20 on Ethereum) (Cousaert et al., 2022). This mechanism is, among others, used in yield farming, which is currently by far the most used practice to invest assets in DeFi, where DeFi's composability enables the usage of tokens across multiple layers of DApps, resulting in multiple yield sources. This composability is one of the main drivers for the success of yield farming. Mmoreover, yield farming is a large contributor to the growth of the DeFi ecosystem (Derviz et al., 2021; Silberholz & Di Wu, 2021; Wachter et al., 2021).

It is also possible to benefit from classic revenue streams in the cryptocurrency ecosystem by participating in the network as a validation node. Native currencies, such as ETH and BTC, originate directly from the blockchain layer, as they are generated in the process of the consensus finding as part of the incentivization mechanism, ensuring the respective blockchain's security (e.g., PoW, PoS, etc.). When having fulfilled the requirements (e.g., providing computational power for PoW or locking stake for PoS), one can participate in the block validation process, which can also be a profitable investment (Binance, 2022; Vermaak, 2022a). Due to its origin and the need to use it as a basic payment currency for the settlement of transactions, native currencies represent an investment in the overall performance of the respective DeFi platform. As the popularity of a blockchain platform increases, so does the need for transactions, and with it the demand for native currency and its value (Corbet et al., 2021). Native tokens can also be of use in DApps by "shifting" them from the native layer to the application layer in the course of a wrapping process. Wrapping native assets, e.g., ETH to WETH, is realized by locking a native cryptocurrency in a dedicated smart contract and simultaneously minting the respective amount on the smart contract layer. This process is also an example for splitting assets into different functions, as we illustrated already above with the example of splitting voting rights from governance tokens. While the native asset represents the utility token of the network, i.e., as fuel to pay transaction fees, the wrapped version of this token enables the utilization of the asset for DeFi applications.

4.3 Fractional Ownership

Ownership in TradFi is a concept of legal possession and control over an object (tangible or intangible) that is deemed property of someone or something. This involves the law and legal system, especially when determining the status of ownership in case of a dispute and an authority which certifies the ownership. DeFi is more connected to the concept of "technical ownership", enabled by the proof of ownership based on the blockchain's immutable data record and digital signatures (Zetzsche et al., 2020). A token corresponds to an address on the blockchain that "owns" tokens until spent. Whoever has access to this address – i.e., whoever holds the corresponding private key – can dispose freely of this token, resulting in a technical ownership via blockchain. This mechanism lays the groundwork for the DeFi ecosystem, making a decentralized financial system possible. DeFi provides accounts on which value is stored on the settlement layer and where ownership is verified and transferred by the rules of the blockchain network. More interesting, but also significantly more complex, is tying the ownership of off-chain assets to these tokens that are tradable in DeFi.

The ability to create different types of tokens based on their level of fungibility allows these tokens to represent items such as unique artworks, vouchers, and tickets on the blockchain, which can then be "owned" by simply storing their digital representation at the user's own blockchain address. Because of the immutable record of the blockchain and its ownership mechanism, it is possible to check for the authenticity of the token by creator address. In this light, the blockchain ensures that the current token holder really owns the respective tokens (Sunyaev et al., 2021). This is especially interesting for the digital art industry, as digital originals of artworks are hard to establish because data can be duplicated and the artworks thus be copied. NFTs, however, have the potential to enable such digital originals that can be owned and not duplicated since the ownership track is documented on the blockchain (Kugler, 2021; McConaghy et al., 2017). Nonetheless, in this case, the original creation of an NFT and the certification that this is in fact the only legitimate tokenization of a specific real-world asset is a single point of failure and only works when real-world trust in institutions or individuals can be transferred to the blockchain ecosystem (Barbereau et al., 2022a). To this end, certificate-based digital identities may play a crucial role (Sedlmeir et al., 2022).

NFTs are also used for decentralized gaming (e.g., Ubisoft Quartz), where items earned by playing can now be owned and traded as tokens on a market amongst players instead of just being items that are rigidly bound to a player's account (Blockonomist, 2021). In addition, NFTs offer properties that could be useful for the ticketing industry by being a representation of an on-chain ticket with easily verifiable ownership history (Regner et al., 2019). However, many challenges in the ticketing industry – such as secondary market control – can arguably not be solved with NFTs alone and instead require strong identity binding to be enforceable (Feulner et al., 2022b).

The concept of fractional ownership can also be easily realized in DeFi. Ownership is "fractionalized" when the underlying asset is split into shares or other titles. A classic TradFi example would be the issuance of stock shares for companies or partial ownership of real-estate through several companies or individuals. In the DeFi-space, such an equal share can be represented by a fungible token. It represents the partial ownership of the underlying smart contract. This smart contract, in turn, can be used to represent an asset. These kinds of tokens can be traded for value on crypto exchanges, with their value connected to the company's success, and can often represent voting rights in company decisions. The associated smart contracts also offer the opportunity to tokenize assets by incorporating an asset into the smart contract and subsequently creating tokens that represent ownership of the smart contract and therefore the underlying asset. The ownership can be sold as a whole, but smart contracts also offer the opportunity to issue fungible tokens or NFTs to represent ownership of fungible or nun-fungible fractions of the tokenized asset.

Assets that have been tokenized already can be further fractionalized or conjoined. This is due to the feature that smart contracts can take over the role of a token owner. Ownership of an NFT, for example, can thus be transferred to another smart contract that releases fungible tokens to fractionalize the NFTs it owns (APYSwap, 2021; FundiFinance, 2021). All these features allow for fast and easy fractionalization, but also the transfer of corresponding partial ownership of digital assets within the DeFi space.

The ownership mechanisms thus can extend, support, or maybe even replace legal ownership through technical ownership, facilitated by cryptographic proofs of ownership based on a decentralized, public ledger. As ownership and possession are crucial aspects in most industries, DeFi bears the potential to ease and accelerate the process of transferring ownership and property (especially internationally). Smart contracts could reduce the bureaucracy involved, particularly, replacing often lengthy and complex procedures of drafting legal contracts and documents in form of a transaction. This transaction includes the ownership-bearing token that settles instantly, irrevocably, and verifiably on the blockchain (Zetzsche et al., 2020).

4.4 Open Systems and Interfaces

Open systems and interfaces typically refers to the inherent properties of transparency, modularity, and interoperability of the DeFi ecosystem. DeFi is mainly enabled by public blockchains, e.g., Ethereum, Solana, or Cardano, and allows for the deployment of individual smart contracts. Since anyone can deploy smart contracts and create new services, the development of DeFi is open to the broad (technically literate) public. Major parts of DeFi are based on open-source code: smart contract code is even required to be publicly visible on the blockchain. Otherwise, trustless, replicated execution would hardly be possible (Schär, 2021). Although DeFi's degree of decentralization in terms of market competition varies on the application level, the open-source availability and transparency of the infrastructure layer could help to achieve sufficient decentralization in the long run (Schrepel & Buterin, 2020). The possibility for "copy-paste solutions" prevents the exploitation of monopolies – for instance, by raising fees – since the opportunity of just copying the code and deploying the same service with lower fees always exists. This leads to competition inherently originating from DeFi's foundation, which drives innovation of new applications. Hence, this can be viewed as a good way to enforce antitrust by technological means and help to address antitrust issues. In this light, DeFi's infrastructure on which the protocols are stored and executed can be considered as shared "public good" that counters infrastructure monopolies. Nonetheless, considering today's market dominance of user interfaces like Metamask or CEXes like Coinbase, where the core software is not smart contract based, it remains a question whether there are significant improvements in decentralization compared to TradFi (see also Section 5).

In any case, decentralization on DeFi markets is rarely enforced at all cost. Similar to how antitrust laws accept the outcome of "healthy" centralization through competition, the DeFi community accepts centralization if it is an outcome of market competition, for example, when a product has an advantage over the products of competitors.[3] For instance, despite the transparency of smart contract code, user interfaces often remain proprietary and can, therefore, exhibit some degree of user lock-in. In other cases, incumbent exchanges may have a significant competitive advantage when they have reached a certain amount of liquidity. Overall, this open ecosystem can make participating in the markets of DeFi as an enterprise for financial services a worthwhile endeavor, since it presents a leveled battleground for competing products. In addition, it offers a fruitful ground for innovations, which can be for the common good of the enterprise and its customers.

For developing DApps in DeFi, there are API providers such as Infura, which offer access to nodes on the respective blockchain network or provide test nets. In combination with other DApps' APIs (e.g., the Compound API and the UniSwap API), this allows developers to create new DeFi applications on an already existing backend or to develop their own backend smart contracts. Due to the modularity of the protocols and applications, companies can also provide entirely new services by combining already existing services in a useful manner. For example, yield aggregators combine different lending, liquidity, and staking pools.

The open-source development in DeFi naturally also corresponds to the auditability of the whole ecosystem. Transactions and smart contract protocol code are published transparently in the P2P network and can be viewed by everyone[4]. In addition, there is the potential of easing and partly automating processes like taxation and auditing by integrating them into DeFi, which are often regarded intricate and lengthy processes in TradFi (Bennett et al.,

[3] See DeFi DApp dominance.
[4] For example, see Etherscan.

2020). On the other hand, public visibility of code also allows attackers to find and exploit vulnerabilities more easily.

The programmability and modularity of DeFi could also influence the traditional financial sectors with different degrees of modification of DeFi-native protocols. A direct usage of DeFi protocols could be possible where banks would conduct their own business operations on DeFi platforms. In addition, they could act as intermediaries between their customers and DeFi protocols, therefore, integrating DeFi directly into their business models. Another implication of DeFi includes a need for its inherent programmability, automatability, and modularity. This does not have to result in banks fully integrating DeFi protocols into their service offering, but could initiate a change in banking business models holistically. In order to stay competitive with DeFi systems, banks could offer APIs that are more versatile and allow the user to automate its interaction with the bank and its services. In order to achieve this, banks might take existing DeFi protocols and transfer them to an open or permissioned systems, which could be managed by the bank or a consortium of banks. Another possibility would be for banks to program their own application or adjust their services to facilitate the programmability. No matter whether banks integrate DeFi protocols directly into their system or just change the accessibility and programmability of their services, DeFi could be a driver of innovation in TradFi.

4.5 Catalyst for New Ecosystems

As shown, DeFi offers great potential for the future of finance and will potentially affect the process of how individuals and businesses engage in financial services. In this view, DeFi can be a catalyst for the creation of a new ecosystem in which DeFi itself is the main provider of decentralized financial services or provides the financial infrastructure for other ecosystems.

Building a bridge between TradFi and DeFi will arguably play a vital role in the further development of finance (Derviz et al., 2021; Lockl & Stoetzer, 2021). Thus, creating such points of convergence that make moving between the two paradigms of finance convenient for users and compliant with regulations, may offer new business opportunities and allow DeFi to overcome some major challenges (see Section 5). This new financial service ecosystem at the intersection is also known as centralized decentralized finance (CeDeFi) (Coinmarketcap, 2022a). In addition, CEXes offer on- and off-ramps from TradFi to DeFi and vice-versa, and as such they are an obvious point for initiating some momentum of convergence (Qin et al., 2021a). Most of the big CEXes also started offering services tailored for institutional investors.[5] CEX are often licensed in multiple jurisdictions in which they provide services. For example, these companies may be registered as money service businesses with Financial Crimes Enforcement Network (FinCEN) in the US or the German Federal Financial Supervisory Authority (BaFin) and need to comply with AML and CFT regulations. Furthermore, there are blockchain forensics companies like Chainalysis and CipherTrace that offer services to crypto businesses, institutional investors, and governments (Binance, 2021). Similar to exchanges, DeFi applications try to become more attractive for institutional investors (e.g., Aave Pro) (101Blockchains, 2021). Considering the Protocol Sink Thesis (see Section 1), this may offer the opportunity for a new ecosystem of institutionally embedded financial services built on DeFi protocols. These developments towards the convergence of DeFi and TradFi could offer a common good for both approaches to financial systems (Derviz et al., 2021; Lockl & Stoetzer, 2021; Meegan & Koens, 2021).

In addition to impacting the financial service industry directly, DeFi could be a catalyst for many more industries by providing a commonly accepted infrastructure for enabling a decentralized governance of digital platforms using DAOs (Wright, 2021). Thus, DeFi may facilitate fluid organizations and the emergence of new forms of business entities (Schirrmacher et al., 2021). Prominent exam-

[5] For example, see Binance, Coinbase, or Kraken.

ples for this is BisqDAO, which is a DAO operating and governing the Bisq DEX on top of Bitcoin. In addition, the DAI stablecoin ecosystem managed by MakerDAO on top of Ethereum falls into this category. These constructs are often not registered as companies or legal entities. In fact, DAOs consist of a variety of smart contracts that are required for their business on-chain and smart contracts for executing decentralized governance (Barbereau et al., 2022b). These entities enable broadly accessible digital and transparent cooperation for various purposes, such as (fractional) ownership and managing complex financial service operations (Wright, 2021). However, as DAOs and DeFi are relatively new developments that come along with regulatory uncertainty, the convergence of TradFi and DeFi can be achieved by, for example, registering the DAO as a legal entity (Mienert, 2021). Indeed, there are already some DAOs that are legally registered entities, such as BlocksDAO and American CryptoFed DAO.[6]

Furthermore, the fragmentation of TradFi struggles to provide a solution for a particular challenge in markets, known as "tragedy of the commons": internalizing and pricing negative externalities (International Monetary Fund, 2020). This problem often needs to be corrected later on by governments via taxation or contingencies. Carbon dioxide emissions are such an externality, because the "cost of pollution" is typically not inherently priced into products. If tackled by contingencies, carbon dioxide emissions are regulated by a central authority that imposes a maximum of carbon emissions via distribution of carbon certificates. These certificates are tradable and offer companies that have not used up their contingency the option to earn money by selling them on a carbon credit market, while providing others whose needs exceed their contingency to obtain more certificates (German Federal Government, 2020). In TradFi, there are unsolved issues regarding greenwashing, fragmented markets, and double spending of certificates (Miltenberger et al., 2021; Sedlmeir et al., 2021c). DeFi, with its interoperable and transparent open-source infrastructure, hereby may provide opportunities to enable envisioned carbon credit markets by means of NFTs as carbon certificates (Khan & Ahmad, 2022). In this context, uniting various stakeholders on a common neutral platform may help to resolve issues arising from system boundaries. For instance, while carbon certificates are used for the compliance carbon market (i.e., required by law), KlimaDAO engages in the voluntary carbon market where carbon offsets are traded. Carbon offsets are produced when carbon dioxide emission is reduced, and as such can be tokenized and made tradable by carbon offset credits to offset produced emissions (Carbon Offset Guide, 2022). KlimaDAO backs their interoperable and fungible "Klima-token" with these offset credits, and thus integrates the negative externalities directly into an alternative currency. In addition, KlimaDAO incoproates it into DeFi markets, which is envisioned to be a promising way to internalize the negative externality of carbon emission (D. B. Chen et al., 2019; KlimaDAO, 2022). On the other hand, as we already indicated in Section 3 and as we will further elaborate on in Section 5, the feed-in of reliable information to create tokenized representations of emissions will unlikely be solved through a DeFi-powered approach. Also, the challenge to make large international stakeholders participate despite obvious financial obligations will be difficult to achieve even with a DeFi-based approach.

Eventually, DeFi comprises the potential of creating an integrative virtual world, also often referred to as the "Metaverse". The Metaverse is expected to be the next mega-phase of the internet by merging physical, augmented, and virtual reality in a shared online space in which users can interact with each other and software applications in a three-dimensional virtual space (Haihan et al., 2021). The goal is to provide a fully fledged economy that offers unprecedented interoperability. This means that users can take their avatars and items from one place in the Metaverse to another without any frictions, no matter who runs that particular platform (Ball, 2021). DeFi might enable this embod-

[6] For reference, see Blocks DAO LLC and American CryptoFed DAO LLC.

ied internet to be independent of centralized platforms and software providers, as DeFi-based tokens and other possibilities may enable the operation of the metaverse in a decentralized way (Newton, 2021; Ning et al., 2021). For example, NFTs could be used to provide dedicated property rights in infrastructures driven by interactive and intelligent avatars. This means that NFTs-based avatars may be able to represent interactive media objects with personality traits and preferences while providing real-time interaction capabilities (Lau, 2022).

5 Challenges

5 Challenges

Although, DeFi has the potential to improve existing or facilitate novel and disruptive financial products and services, it is still in its infancy and therefore faces great challenges. The emerging ecosystem is highly vulnerable from a technological, financial, and regulatory perspective. It remains an open question whether DeFi will overcome current challenges and evolve into a mature ecosystem that can be beneficial to the economy, businesses, and society. The following section highlights the main risks and challenges that DeFi is currently facing. It also suggests potential or pursued approaches to address these problems.

5.1 Technical Risks and Security Concerns

Most importantly, DeFi needs to address several technical and particularly security concerns that are closely related to its layered architecture and infrastructure. Technical risks are one of the most fundamental issues and endanger the entire DeFi ecosystem if not addressed properly.

As DeFi is an open and permissionless environment, everybody can deploy their smart contracts. Consequently, the quality of protocols might differ substantially between different services. Even when smart contracts have been tested and quality-assessed, experience shows that there is always the possibility of errors and bugs in the code, even in smart contracts of big DeFi services, as illustrated by the infamous "DAO hack". This hack exploited a coding error that affected the wallet smart contract of the DAO. In detail, when executing the split function of the DAO in a first step, the ETH was withdrawn and only in a second step the internal balance was updated accordingly (Daian, 2016; Dhillon et al., 2017). In 2016, this flaw allowed a hacker to siphon off multiples of the initial deposited funds by recursive call exploits.[7] 3,641,694 ETH (approximately 14 % of all ETH in circulation at the time) were stolen, which ultimately led to a hardfork of the Ethereum blockchain by excluding the malicious transactions (Cryptopedia, 2022; U.S. Securities and Exchange Commission, 2017). Another severe example of a hack affecting wallet smart contracts is represented by the recent hack of the cross-chain network "Poly Network", in which approx. USD 600 million (value in cryptocurrencies) were stolen by gaining control over the wallet smart contracts through flawed code (Gagliardoni, 2021). However, in this example, several blockchains were attacked in a cross-chain network, which is one of the reasons why the attack could not be reverted, like in the case of the DAO hack. Yet, it is not clear whether a hard fork would be accepted even on a single major chain nowadays. There are a plethora of examples across different DeFi services exhibiting smart contracts flaws and bugs that have been exploited over the years. Hence, loopholes and flaws in code pose a real, costly, and persistent risk in the DeFi space.[8]

Another security-related aspect is end users' cryptographic key management. As funds are stored on the blockchain and are only accessible by the corresponding private key, the access to these keys should be well secured. There are two main categories of wallets: custodial wallets and non-custodial wallets. In non-custodial wallets, end-user control their private keys. In custodial wallets, a third party manages the private key and maintains account balances of the end-users. End-users typically authenticate with such services through usernames and passwords. Typical custodial wallets are accounts at a CEX, which manage a lot of funds, making them an attractive target for attacks (Merkle Science, 2019; Song, 2017). CEX wallet security is an important step towards minimizing risks for a significant amount of funds in DeFi, which needs yet to be sufficiently addressed (Huili et al., 2021; Suga et al., 2020). However, custodial wallets provide access to funds in case of a forgotten password. In contrast, users storing their private keys by themselves are independent of centralized

[7] See Open letter of the attacker.

[8] For further information, see Balancer attack, Bisq attack and bZx attack.

service providers. Noteworthy, these users take the responsibility for their keys, implying much higher risk in case of losing access to the wallet and funds become forever inaccessible (CBC/Radio-Canada, 2021).

Being unable to rescue funds is a common risk in DeFi due to its decentralization, which leaves no single authority that could possibly reorganize the database to rescue funds. The reorganization needs to be decided in a complicated process by the whole network and often ends in a fork of the blockchain, since not everyone agrees, as in the example of Ethereum and Ethereum Classic. In addition, DeFi comprises an adversarial environment and even transactions aiming to rescue threatened funds can be frontrunned (typically by automated bots) and the funds still stolen (Robinson & Konstantopoulos, 2020; Werner et al., 2021). Eventually, the transparency of the blockchain is only useful to a certain degree for tracing attackers. The DeFi ecosystem provides sophisticated services such as mixers, e.g., Tornado Cash, or other anonymity-enhancing tools to obfuscate the origin of transactions (see Subsection 5.4).

DeFi is also exposed to "flashloan attacks" (Vermaak, 2022b). As explained in Section 2, primarily, flashloans are not meant as a means of attack, but rather to carry out trades more efficiently. Nonetheless, they can represent a tool for attackers to reduce the entry barriers for conducting attacks on smart contracts to which they would be vulnerable even without involvement of flashloans, e.g., oracle attacks, pump and arbitrage, bug exploits, or frontrunning (Cao et al., 2021; Gudgeon et al., 2020a). As a tool for attacks, flashloans provide two important features: First, they are atomic, i.e., they execute a series of transactions that cannot be interrupted. Second, the money that one has to input is reduced to the flashloan's service fee, which in turn provides the necessary amount of funds to conduct the attack. Overall, it is observable that floashloans allow attacks to be more profitable and less risky (Qin et al., 2020; L. Zhou et al., 2021). Since flashloans are a tool for particular purposes, such as arbitrage, they are a double-edged sword in DeFi. However, DeFi services can protect themselves from being attacked through flash loans, e.g., by prohibiting flashloan functionality or considering potential attack vectors and implementing measures to eliminate them, such as a maximum flashloan amount (Gudgeon et al., 2020a; Qin et al., 2020).

5.2 Scalability Issues

Scalability issues have a direct impact on the DeFi ecosystem. Most DeFi platforms can only process a few transactions per second, e.g., approximately 15 tx/s on Ethereum. In times of high throughput, this leads to congestion and, consequently, higher transaction confirmation latencies. Specifically for small investments, high transaction fees could make DeFi's declared goal of improving financial inclusion unattainable. Further, many DeFi transactions that are appealing for institutional investors are more complex than a simple payment and therefore can be prohibitively expensive. To mitigate the risk of being frontrunned or to avoid large slippage in AMMs that would make a trade less favorable, large trades often need to be split into many smaller trades distributed over a larger period of time. This splitting further increases scalability requirements, transaction fees, and latency concerns. However, there are several approaches to address scalability challenges:

- Move the application to another blockchain that does not prioritize decentralization. By demanding high-performance hardware and high bandwidth, these systems can reach a much higher throughput and sub-second latencies (Sedlmeir et al., 2021a). A popular example is Solana. However, such systems are also more centralized and empirically seem to have frequent issues with networking incidents and denial of service attacks (Reguerra, 2022). Often, moving to other blockchains comes along with trade-offs in terms of throughput, transaction fees, latency, and decentralization. In addition, it requires creating bridges to other DeFi platforms like Ethereum. Bridges are needed so to exchange assets cross-chain and leverage liquidity of established DeFi platforms. However, this bears considerable security risks, as bridges are complex and, thus, error-prone. Hackers can target the bridge smart contracts on either side. They can also directly attack the consensus on the more vulnerable chain involved, as for example, the recent Poly Network hack illustrates (Gagliardoni, 2021).

- Increasing the performance of the base layer by optimizations of computation and storage costs and by introducing scalable side-chains. In this view, concepts like sharding reduce the degree of redundancy in transaction storage and execution. For example, Ethereum 2.0 will presumably have 64 shards for data availability, which helps to increase the throughput by around the same factor (Ethereum Foundation, 2021). Since sharding carries a tradeoff in terms of the degree of redundancy and, thus, cross-checks on a blockchain, the number of shards needs to remain rather limited. Therefor, shards can only add a small factor in terms of throughput.
- Implementing so-called ”layer two” (L2) solutions to increase transaction speed and scalability. L2 systems do not store or process all relevant information on the underlying blockchain and, therefore, reduce the overall capacity requirements of the DApps connected to the L2. Nonetheless, the L2 solutions are designed in a way that makes them benefit from full integrity and availability guarantees of the underlying blockchain (Monolith, 2021). The most popular variant are rollups that use domain-specific optimizations to reduce the required storage. In addition, rollups take some of the transaction-related information and a major share of the computational effort off-chain. On the one hand, there are optimistic rollups where presumably “wrong” computation can be challenged and punished on-chain; this approach is conceptually easier but also implies longer latencies (typically, a week) or additional services (liquidity providers that accept a small risk) for withdrawals. Consequently, liquidity is used less efficiently. On the other hand, zk-rollups prove the correctness of the off-chain accounting through cryptographic proofs, usually ZKPs (Gluchowski, 2019). This short (“succinct”) proof is then checked by a smart contract. This approach is more complex, but an increasing number of initiatives are successfully launching zk-rollups that cover increasingly complex transactions: While early zk-rollups only supported payments in the native currency, more recent implementations cover transfers of ERC-20 tokens. There is ongoing work to support arbitrary smart contract functionality. Both optimistic and zk-rollups face centralized operations, but prevent the need for centralized trust. The security of funds is as good as the security of the blockchain settlement layer, and withdrawals can be made even if the operator ceases to provide its service. With rollups, depending on the required confidence in data availability guarantees, throughput can be increased by a factor of several hundred to tens of thousands of the base throughput (Schaffner, 2021). At present, various rollups are already live on the public Ethereum blockchain; and while they are not yet operating at their capacity limit, they already offer reductions in transaction fees by one to three orders of magnitude. Thus, rollups have experienced an increasing rate of adoption, lately.

5.3 Illiquidity

Providing sufficient liquidity poses a major challenge for all kinds of financial markets. These markets play a key role in ensuring their usability and efficiency. While most traditional markets solve this problem by having centralized intermediaries acting as counterparties or market makers, the DeFi ecosystem needs to rely on other mechanisms to attract liquidity. Liquidity ensures the functionality of and enables further adoption in DeFi, especially from institutions.

In general, liquidity plays a particularly important role for exchanges, as their usability and the volume of trades that can be settled depending on the available liquidity on the exchange and in the market. Traditional exchanges and brokers hence use market makers that ensure sufficient liquidity and act as a counterparty for incoming trades to provide users with fast trade execution and low spread. Since DeFi, by its nature, lacks these centralized parties, most trades are executed through AMMs. In addition, DeFi protocols provide instantaneous trade execution owing to the existing liquidity pool acting as a counterparty. Thus, the spread that is paid by users mainly depends on the ratio between the trade size and the size of the liquidity pool (Pourpouneh et al., 2020). This is why the size of liquidity is one of the most important criteria in the competition among AMMs: the higher the liquidity, the lower the trader's spread. Furthermore, liquidity is not only an important competitive factor for AMMs but also for stablecoins. Since the goal of a stablecoin is to maintain its value, a big spread, especially when trading one stablecoin against another, can be very inefficient. Consequently, large amounts of liquidity can also act as a (short-termed) mechanism for stablecoins to hold their peg.

Moreover, especially in DeFi, liquidity is not only important for trading efficiency but also for the functionality of other applications such as lending protocols. To ensure the usability and efficiency of lending protocols, sufficient liquidity on both the supply and the demand side is required. A lack of demand results in low interest rates for suppliers, while a lack of supply can result in suppliers not being able to withdraw funds (Gudgeon et al., 2020b).

While some risks are isolated and only affect one DeFi application, others can spread through different ecosystems although limited to one DeFi application (e.g., the hack of the cross-chain network). Specifically, wrapping and collateralization processes can amplify risks through liquidation processes that occur in the case of an incident, or can make risks more difficult to trace. Similar to how the cross-chain network acts as an oracle between different blockchains, there are oracles that intermediate between different DeFi applications on one blockchain (e.g., AMMs as price oracles for other protocols). Exploits of these channels between different protocols already exist, where flaws in the code of one protocol are exploited to attack another that relies on its functionality (e.g., bZx pump and arbitrage attack, the bZx oracle attack, the balancer attack, etc.) (Cao et al., 2021).

Another dimension of this "composability problem" becomes apparent when considering that these protocols are not only connected by their functions for each other but also by their assets (e.g. through wrapping or relying on collateral). For example, if a stablecoin which is used in a variety of DeFi protocols fails to maintain its peg and faces a drop in value, all linked protocols that are affected likewise. An example for this may be a chain of liquidations spanning throughout the DeFi ecosystem, resulting in undercollateralization of lending pools (Gudgeon et al., 2020a; Meegan & Koens, 2021). Channels and mechanisms like wrapping through liquidity mining and yield farming can therefore help to spread the risk to various DeFi applications and platforms, leading to the downfall of the whole DeFi ecosystem. This is often referred to as systematic risk. For example, the initial de-peg of the UST stablecoin and the downfall of the Terra ecosystem lead to exchange rate losses of other currencies, liquidations, and illiquidity of multiple DeFi service institutions. The UST example provides a foretaste on how these inhibit risks can affect the entire DeFi ecosystem (CoinDesk, 2022a, 2022b, 2022c). In addition, problems can arise from code flaws that is typically copied and used as building block for new DeFi services in an open source environment (e.g., Sushi Swap as a fork of Uni Swap). Hence, flaws in the original code would be duplicated multiple times, contributing to destabilization and increasing systematic risks in DeFi (Schär, 2021).

Additionally, there is also a systemic risk in DeFi's infrastructure layer, i.e., in case the blockchain is compromised (Schär, 2021). Each risk that menaces the integrity and functionality of the settlement layer endangers the functionality of the DeFi services on top of it, thereby, leveraging systemic and creating systematic risk. For example, exploiting or breaking the consensus mechanism using sophisticated technology like quantum computing or a centralized block production can facilitate a 51 % attack on the network (Aponte-Novoa et al., 2021; Fedorov et al., 2018; Guggenberger et al., 2021b).

It is important to recognize the interplay between these technological and economical risks: To prevent illiquidity in protocols, it may be necessary to further increase incentives to supply liquidity. These incentives might have detrimental effects on currency-based consensus mechanisms, e.g., PoS, and thus undermine the security of the blockchain (ConsenSys, 2020; Stevens, 2020). Yet, finding a healthy balance in this trade-off represents a crucial challenge.

5.4 Transparency vs. Privacy

As we described in Section 2, one of the fundamental properties of a blockchain is the redundant storage and execution of transactions. Besides providing transparency and trust in the correct processing of transactions, this property implies two major challenges.

The publicly visible transaction history impairs individuals and organizations, as sensitive information is stored transparently (Sedlmeir et al., 2022). For example, CEXes can use metadata based on KYC processes, patterns, habits, and business information to establish a link to a person despite the pseudonymization that most blockchains offer (Biryukov & Tikhomirov, 2019; Hickey & Harrigan, 2021). This also bears the risk of breaching data protection regulations (e.g., the General Data Protection Regulation (GDPR)) for personal data, or anti-trust regulations for business data (Rieger et al., 2019; Schellinger et al., 2022b; Sedlmeir et al., 2022). For example, competitors can observe an organizations' financial transactions and risks involved when acting on a DeFi platform. These challenges can generally be addressed using cryptographic privacy-enhancing technologies like ZKPs. ZKPs are already being used for anonymizing transactions, e.g., in the Ethereum-based mixer Tornado Cash (Sun et al., 2021). Consequently, blockchain-based applications, such as data markets, specifically require privacy-enhancing technologies (Munilla Garrido et al., 2021).

Apart from privacy issues, there are direct economic challenges that are caused by the transparent execution of transactions. Through the initial distribution of all transaction information in the mempool (see section 2), block-producing nodes can automatically check whether they can make additional profit from inserting own transactions in front or thereafter (Eskandari et al., 2019). This phenomenon is called "extractable value" and one of the most popular examples are frontrunning attacks. For example, an arbitrage trader identifies a large transaction order on a DEX that is to considerably increase the price of a specific token and can frontrun by initiating a transaction in which the block producer buys the same asset. Simultaneously, the arbitrageur sells the asset after the "big" transaction, receiving a profit in the form of the margin. These "sandwich attacks" have been observed frequently in DeFi (Werner et al., 2021). Not surprisingly, they are legally forbidden for brokers in TradFi (Financial Industry Regulatory Authority, 2013). Usually, these attacks lead to a competitive game of transaction fee bidding between the attackers, which may render the attack unprofitable if there is a large amount of attackers participating (Qin et al., 2021b). However, if the extractable revenues are higher than the "normal" block reward, there are incentives for block producers to benefit from this situation. Block producers can circumvent the fee bidding by just including their transaction in front of the target transaction, resulting in a competitive game of reorganizing the blockchain. Effectively, frontrunning weakens the consensus and, thus, represents a systemic risk (Daian et al., 2020; Qin et al., 2021b). Several approaches to solving this problem are currently being explored. One approach, brought by organizations like Flashbots. This company aims to reduce information asymmetries through tools that users can use to check if and to what extent they can be frontrun. An alternative is the conditional operation of transactions by putting restrictions ("slippage tolerance") on the market price clients are willing to pay in a DEX transaction. While both of these approaches have limitations regarding the generality of transactions, they offer a remedy to these "value extraction attacks" (Qin et al., 2021b).

"Gradual decryption" is a viable solution to miner extractable value (MEV) and represents a rather generic approach in systems where a set of validators (potentially pre-selected in PoW or PoS) is responsible for consensus: transactions are encrypted with an aggregate epoch public key in the mempool and also remain encrypted during the block production process. They can only be decrypted gradually after being committed on the blockchain and partially confirmed (and partly decrypted) by validators, so the block producer cannot see the transaction details and is unable to develop a way to "sandwich" the transaction (Bebel & Ojha, 2022; Kursawe, 2021).

Despite the fact that many transactions can be traced back to an individual or organization (e.g., companies like Chainalysis offer such services), there is also a need to address AML and CFT regulation; specifically when privacy is enhanced as a response to the previously mentioned challenges. DeFi and alternative digital assets in general will also require audit trails so that organizations can prove compliance with regulation or disclosure of all transactions in their tax declaration. Overall, we see two major implications of this tension between privacy considerations on the one hand and regulatory demand for transparency on the other hand: There is a need for "selective privacy", where only the minimum information needs to be disclosed for regulatory compliance is stored on-chain. In this light, ZKPs can prove the legitimacy of transactions while only selectively disclosing inputs and outputs or properties derived from them. Therefore, ZKPs can be a viable cryptographic tool for achieving selective privacy (Barbereau et al., 2022a). Moreover, for interactions with real-world identities from the regulated domain, a certificate-based digital ID will need to interact with on-chain smart contracts to prove legal age or an authority's confirmation of approval of a certain transaction. For this purpose, again, selective privacy is crucial, for example, to hide the identity of the individual or organization that proves the possession of a certificate attesting the legality of the transaction. In this context, certificate-based digital identities with predicate proofs through zero-knowledge technology may be particularly helpful (Sedlmeir et al., 2021b).

5.5 Lack of Harmonized Regulation

Regulatory uncertainty refers to a set of problems resulting from the circumstance that many existing financial regulations cannot just be transferred from existing financial systems and products to this new evolving ecosystem, but instead adjustments have to be made, or new regulations have to be elaborated from scratch. Indeed, many illegitimate activities that have been banned from financial markets through regulation in the last centuries can now be seen in DeFi as it catches up to the century-long development of traditional financial markets.

There are already many proposals and laws aimed at regulating virtual assets in different jurisdictions that also concern DeFi services. These legislations can be divided into two categories. The first category includes supranational law, such as markets in crypto assets (MiCA) and anti-money laundering directives (AMLDs) of the European Union (EU), Crypto-Asset Reporting Framework (CARF) of the Organisation for Economic Co-operation and Development (OECD), and guidelines of the Financial Action Task Force on Money Laundering (FATF), that instituted by transnational organizations. The second category are national laws, such as different tax (e.g., income tax and value-added tax) and supervisory laws (e.g., banking acts and payment services acts). Often, the supranational proposals are adopted in the individual member countries by incorporating them into national laws. Yet, the implementation might vary between different countries.

For example, the FATF is an institution that sets international standards aiming to fight money-laundering, terrorist financing, wash trading, and other market manipulations in virtual asset markets (Financial Action Task Force, 2022). Every legal or natural person, that offers services that involve virtual assets, is thereby considered a virtual asset service provider (VASP). Even the technology (e.g., smart contracts, DAOs, or DApps) and everyone that is involved with this "intermediary technology" (e.g., owners, operators, and founders) may be classified as VASP (Financial Action Task Force, 2021). The classification requires reporting KYC and other information to national authorities, the authorization by licensing and registering its service within every of its jurisdictions, and further compliance with regulations like the "traveler's rule"[9]. Although the guidance of the FATF does not exhibit a legally-binding character, it is expected that a multitude of nations will adopt versions of the proposal in their national laws (Ferreira, 2021).

The implementation of these proposals and the responsible authority depends on the type of token. For example, businesses issuing security tokens can be registered with the Securities Exchange Comission (SEC), while activities concerning commodity- and future-like tokens may be registered with the Commodity Futures Trading Commission (CFTC), whereas stablecoin businesses may be overseen by the FinCEN (U.S. Securities and Exchange Commission, 2019). A similar distinction can be observed with MiCA (European Union, 2019). Therefore, lawmakers and regulators in many cases can expand existing laws to include new types of financial service providers by linking them to standards that apply to traditional financial institutions. Thus, some tokens can be designated as direct stock purchases (DSPs) and respective service providers regulated by securities exchange commissions, e.g., the SEC and Federal Election Commission (FEC) (U.S. Securities and Exchange Commission, 2022).

However, regulatory obligations can only apply if the activity, i.e., the credit business, is regulated. For example, the German Banking Act refers exclusively to the granting of loans in fiat currencies and not to the lending of crypto assets. Individuals that provide loans on dedicated DeFi lending platforms will probably not be subject to licensing since they do not know the identity of their counterpart (Auffenberg, 2022). An administrator of the smart contract could, however, be subject to authorization as a crypto custodian on an individual basis as a result of the receiving, holding, and managing of crypto assets. Cryptocurrency custody businesses include the custody, management, or the safeguarding of private keys and thus are required to be authorized by the German financial supervisor. In this light, staking providers meet the legal definition by the German Banking Act of managing crypto assets for others. Hence, they are subject to authorization provided that users delegate their rights to the staking provider service (Auffenberg, 2021).

Owing to the difficulty of overseeing the complex DeFi system from a regulatory perspective, financial institutions like the Financial Stability Board are also afraid that the intertwined components of DeFi could introduce new systematic risks (Catalini et al., 2021). These risks may spill over into the TradFi sector through the growing inter-connectedness (Financial Stability Board, 2022). Beyond systematic risks, protection of financial risks and crime has not yet been implemented in DeFi (Catalini et al., 2021). As a result and besides technical issues associated with this enforcement, the currently fragmented and continuously developing regulatory patchwork contributes to DeFi still operating with minimal KYC, AML, and CFT checks, thereby exhibiting a significant deficit in compliance. Regulation can only be enforced on centralized parts of DeFi because identifying and grasping the majority

[9] See Guide to the FATF Travel Rule.

of individuals governing such entities is inherently difficult owing to the pseudonymous and decentralized nature of public blockchains (Schär, 2021). Entities that have on- and off-ramp links (e.g., CEXes or non-custodial stablecoin providers) need to interact with TradFi (e.g., commercial banks) and thus are required by law to be compliant. In addition, they need to ensure accountability before being able to start their businesses operations. Bridging the gap between DeFi and TradFi by integrating trusted financial supervisory bodies on a technical level to centralized endpoints in DeFi poses a potential solution. For example, the introduction of central bank digital currencies (CBDCs) as a compliant form of stablecoins (Bank for International Settlements, 2022; Derviz et al., 2021) or increasing pressure on centralized points, e.g., by demanding admin keys or obtaining voting power (Ushida & Angel, 2021; Zetzsche et al., 2020) can reduce regulatory burdens.

Many current laws are not applicable for DeFi services. In addition, the simplification of tokens into three main categories fails to account for the broad variety of financial instruments in DeFi (Goforth, 2018; Maia & Vieira dos Santos, 2021). With regard to DeFi-based services, traditional regulation through laws is also often unfeasible, since the pseudonymity and decentralization of DeFi often inhibits the enforcement in case of violations. Eventually, DeFi services on a public blockchain are globally accessible and thus stretch over multiple jurisdictions. The process of complying with multiple regulation regimes is a costly burden, further increasing the risk of regulatory arbitrage, and escape of service providers towards more decentralized and difficult-to-regulate platforms (Wright & Meier, 2021).

5.6 Improper Property and Consumer Protection Laws

Prevailing legal frameworks for rights and claims (i.e., legal ownership and possession) as well as for contractual obligations and rights do not sufficiently address DeFi's specific requirements. The classification in common law systems for personal property, i.e., things in possession (TIP) and things in action (TIA), leads to problems, especially regarding cryptocurrencies. They do not classify as TIP because they are data strings recorded on a public ledger and cannot be physically possessed. In addition, they do not classify as TIA, since they do not represent an entitlement to payment against a legal entity (Bolotaeva et al., 2019). An example for a TIA is money in a bank account, as it is an entitlement to payment of tangible money against the bank, while tangible money itself, like banknotes, classifies as a TIP.[10] A cryptocurrency which is technologically owned and possessed by the private key of the address, hence, is neither considered TIP nor TIA. The consequence of crypto assets not being able to be subsumed under one of these categories is that they are not legally recognized as personal property. Consequently, legal methods of protecting property, settling claims of contracts, or enforcing obligations may not apply (Fox, 2018).

However, although legal uncertainty is still the dominating status quo, there have been efforts to reduce this uncertainty, e.g., by Liechtensteins's Tokens and Trustworthy Technologies Service Providers Law (TVTG). The TVTG classifies tokens as a new construct at the intersection of the physical world and digital rights. A token is defined as "a piece of information on a TT System which [...] can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights [...]" (Government of the Principality of Liechtenstein, 2021).[11] The token is designated as a container for rights, which makes various civil rights and property laws in particular applicable, i.e., there is now a legal basis for transactions, trading, ownership or custody (Nägele, 2020). Due to the uncertainty created by the lack of regulations (and their lack of enforceability), scams and other illegal activities are still widespread, as it is difficult for users to distinguish between legitimate products and scams. In addition, the pseudonymity of the system helps scammers in this regard. This

[10] Balance on a custodial wallet represents a TIA against the custodian.

[11] TT stands for "trusted technology".

is detrimental to the user-friendliness of DeFi, as users could face severe losses of their investments through scams and fraud. The transparency of smart contracts, which in theory could prevent most of the scams and attacks, has no substantial effect in practice, as end users typically do not have the time and knowledge to verify their legitimacy. In particular, losses have increased owing to the growing threat of rug pulls that accounted for 37 % of all scam revenues in 2021, amounting to USD 2.8 billion. Rug pulls exploit investors that purchase the scam project's token or provide liquidity to a pool of the token on a DEX. The scammers, which either hold a large percentage of the token or still have control over the entire liquidity pool, then dump all their tokens, thereby siphoning the entire pool (Malwa, 2021). Another widespread danger for users are phishing attacks that aim at acquiring the seed phrases of users wallets and thus obtaining control over the assets in their wallet.

With increasing interest in DeFi, criminals are getting smarter in exploiting the system. For example, the online application Antinalysis allows criminals to check their own Bitcoin wallets and see whether they have any sort of association with criminal activity. One of the most private cryptocurrency used for money laundering in ransomware is Monero. It is estimated that around 10 to 20 % of ransoms are paid in Monero (Ciphertrace, 2021). At the same time, an increasing number of marketplaces that are on the dark web are exclusively accepting cryptocurrencies.

Considering aforementioned regulatory challenges, it is important to find a suitable approach to regulate DeFi without inhibiting its development. Research on DeFi regulation thus proposes multilateral multi-stakeholder approaches, where different parties (e.g, regulators, service providers, and users) of different jurisdictions should be involved in finding a fair solution to the DeFi regulation dilemma (Hughes, 2021; Matsuo, 2020; Takanashi, 2020).

5.7 Inconsistent Taxation and Accounting Rules

Due to the authoritative principle, the term "economic good" under German tax law is identical to the term "asset" under German commercial law. Both terms include not only objects and rights within the meaning of the German private property law, but also actual conditions and possibilities. These terms thus include cryptocurrency, which makes taxation and accounting laws applicable to virtual assets (German Federal Ministry of Finance, 2021). More or less the same applies to other countries, i.e., the US, where cryptocurrency is declared as property for the sake of tax purposes (U.S. Internal Revenue Service, 2022). Regarding taxation of cryptocurrency and gains made in DeFi such as lending and staking, the tax treatment differs from country to country. Often there is no clarity on which category of assets cryptocurrencies belong to, on how critical matters such as taxation of cryptocurrencies gained by hard-forks and staking are treated, and, overall, if and how current laws apply to virtual assets (PricewaterhouseCoopers, 2021).

As crypto assets are not a TIA, they cannot be classified as equity instruments in accounting, and they are not classified as cash because they are not regarded as a medium of exchange and unit of account (International Financial Reporting Standards Foundation, 2019). According to the International Financial Reporting Standards (IFRS), cryptocurrencies, thus, are intangible assets, to be accounted for under International Accounting Standard (IAS) 38 (general intangible assets) and IAS 2 (inventory) depending on different kinds of tokens. The answer to whether asset custody should be reported on or off the balance sheet is not clear. For entities issuing crypto assets (e.g., through ICOs) there may also apply different guidelines based on different kinds of tokens (e.g., IFRS 9 and 15 and IAS 32) (Ernst & Young, 2019; PricewaterhouseCoopers, 2019). Further, accounting principles do not provide clear guidance for reporting of the many varieties of crypto assets (Association of Chartered Certified Accountants, 2022).

5.8 Recentralization

DeFi is based on redundant data storage using blockchains, thus distributing the responsibility of maintaining system integrity among multiple participants in the network. But this does not directly imply that crypto assets and DeFi applications are decentralized at their core. Thus, it is vital to differentiate between the degree of decentralization that is related directly to the blockchain infrastructure and on-chain distribution of tokens coupled to DeFi application's use and governance.

The settlement layer involves two crucial dimensions to be considered to assess the degree of decentralization, namely protocol-level and mining-level decisions. Protocol-level decisions are automatically made by the set of protocols implemented in the client software, while mining-level decisions are decoupled from the protocol and are related to how a new block can be created (P. Zhou, 2020). The former can be evaluated by the number of running full nodes and their geographical distribution. The latter plays a key role in maintaining blockchain security, thus preventing double-spending attacks. It also ensures functionality to avoid censorship of the processing of pending transactions. To achieve a high degree of decentralization, it is important to distribute and disperse the power of producing new blocks. The increasing competition and technological advancement lead to the emergence of numerous mining pools, aggregating hashing power to validate new blocks. In the example of Bitcoin, the combined hashrate for the four largest mining pools (Antpool, Foundry USA, F2Pool, and ViaBTC) over the past year aggregate over 50 %[12] of the hashing power required to attack the network. In total, there were on average 13,911 reachable full nodes in Bitcoin dispersed globally (53.4 % unknown, 12.8 % United States, 8.4 % German).[13] A recent report further emphasized the strong centralization of public blockchains and particularly Bitcoin on multiple levels, including the distribution of hashrate, messaging (concentration on few hosting services, internet service providers and countries), which can become particularly problematic owing to unencrypted messaging and the vulnerability of consensus to increased latency or even package loss (Sultanik et al., 2022).[14] For a comprehensive systematic study of centralization tendencies in cryptocurrencies, we suggest readers to refer to the taxonomy by Sai et al. (2021).

In addition, blockchain-based cryptocurrencies, such as Tether or XRP, have a high degree of centralization owing to their governing bodies. Thus, centralized power results , for example, in manipulations scandals, and can negatively affect the ecosystem as a whole (Griffin & Shams, 2020; U.S. Securities and Exchange Commission, 2020). In contrast, PoS-based blockchains, such as Polkadot or Tezos, seem to be more decentralized, as the integrity of the network relies on the amount of validator stakes. However, the degree of decentralization in PoS-based blockchains considerably depends on the distribution of voting weights and the required hardware components to operate nodes.

The DeFi ecosystem composes applications run by smart contracts that use proprietary tokens to govern protocol decisions and thus set the course of these projects. The governance of DeFi protocols demands a balance between broad token distribution, encouragement of user activity, and the alignment of financial incentives for token holders, users, and the protocol itself (Jensen et al., 2021). Against this backdrop, it is imperative to pay attention to the token ownership distribution of on-chain DeFi applications.

In addition, the control of the team or the protocol over the assets supplied by users plays an important role. For example, in the context of DeFi lending protocols, six degrees of decentralization exist. The degree of control of a project's team be-

[12] See Bitcoin's hashrate distribution.

[13] See Bitcoin node distribution and Ethereum node distribution.

[14] See assessment of this report.

hind a protocols can be measured by evaluating various components, including custody, price feeds, initiation of margin calls, provision of margin call liquidity, interest rate determination, and protocol development (Kistner, 2019). So far, no DeFi protocol is truly decentralized. In general, the distribution of governance tokens among key DeFi applications shows a high concentration, increasing the risk of aggregated power controlling the project (Jensen et al., 2021). Moreover, token holders rarely exercise their voting rights (Barbereau et al., 2022c). What may be even more critical is the current design to grant multiple rights combined and implemented in one token, particularly, economic interests in revenues and voting rights. The combination of these rights makes DeFi protocols prone to governance attacks. Thus, these rights should be decoupled from each other to mitigate risks (Buterin, 2021). To address this issue there are four potential solutions:

- Limit coin-driven governance to reduce the vulnerability of the system being compromised by determined attackers. Instead, use on-chain governance for applications, add time delays, or allow a more fork-friendly protocol. However, governance itself needs to be improved since public good funding, i.e., valuable projects without dedicated business models, is prone to be exploited through bad decisions.
- Use governance techniques that are not coin-voting-driven. Rather base weights on alternative measures, e.g., on verified accounts per human, proof of participation in a system, or a hybrid version of the former two like quadratic voting.
- Increase individual responsibility in voting to break the decision that applies to all. In addition, align individual decisions to their desired outcomes. For example, coins will be destroyed in an attack if an individual votes for the attack.
- Combine aforementioned solutions to move away from coin voting based decentralized governance.

6 Conclusion

6 Conclusion

In light of the presented arguments, we can conclude that DeFi carries great potential as it is built on a neutral platform. DeFi unites a global pool of investors, service providers, and developers that benefit from relatively low entry barriers and potentially high network effects, especially compared to TradFi institutions and services. Potential applications within the DeFi ecosystem offer a significant variety of use cases such as yield farming, insurances, lending and borrowing, collecting and trading NFTs. Therefore, DeFi provides a technology stack that adds new features and opportunities in finance, and moreover, enables the combination of existing and emerging financial services and products, making DeFi highly composable.

Nonetheless, there are still various challenges regarding DeFi's technical implementation, regulatory uncertainties, and the various intersections of these fields. Especially to enable mass-adoption of DeFi, the ecosystem needs to overcome these challenges to fully unleash its potential. In particular, it is necessary to assure that participants can be held accountable to integrate DeFi-based services in existing regulation. In addition, solving economic constraints like ensuring sufficient liquidity as well as technological issues especially regarding scalability is crucial. Besides further advances in blockchain technology, it is imperative to find a balance between on-chain and off-chain processing of information and transactions. In this light, it is important to align the replicated execution with scalability requirements as well as trade-offs between transparency, auditability, and privacy. The spectrum between highly decentralized DeFi ecosystems and more centralized ones allows addressing different stakeholders' and use cases' requirements. Moreover, the differences and interactions between the public and individuals as well as permissionless and permissioned blockchains create an even broader range of alternatives to choose from to find the best fit for individual applications and stakeholders.

DeFi is a new paradigm that may have a strong influence on the future of the financial sector and how people interact with it. While DeFi is a highly innovative space, only the future will tell which of its new applications will remain. Nonetheless, the impact that DeFi already has on the TradFi system is undeniable and cannot be expected to vanish any time soon. DeFi exhibits issues in the TradFi sector in an indirect manner by forming a more efficient and trustless system, therefore highlighting flaws and inefficiencies in TradFi and promoting changes to improve them. We believe that DeFi with its underlying technology and fundamentals will not remove TradFi, but instead will become a trustless and decentralized foundation to the existing financial sector, following the protocol sink thesis. Along the way, the two sectors will keep converging creating a more mature ecosystem with a more complete regulatory framework. Moreover, we might see TradFi-based service providers starting to adopt concepts of DeFi or provide customers with dedicated access to DeFi-based services.

In addition to the influence on the TradFi sector, DeFi acts as a catalyst for a broad range of research and development in blockchain technology. Advances, for example in zero-knowledge technology, have been strongly driven by DeFi projects and are likely to be transferred to other application areas, e.g., in blockchain-based supply chain management. DeFi propelled a high degree of innovation, but the different dimensions of DeFi still require thorough research. In this context, the role of DeFi in the Metaverse might also be a worthwhile endeavor for further analysis. The most important challenges of DeFi, however, involve its complex technical foundations, the legal environment, economic consequences, business opportunities, and user-friendliness. Like many applications in the area of blockchain, interdisciplinary research and close collaboration between academia and practitioners are key.

References

101Blockchains. (2021). Aave pro is ready to onboard institutional investors in DeFi. Retrieved July 14, 2022, from https://101blockchains.com/aave-pro-is-ready-to-onboard-institutional-investors-in-defi/

AAVE. (2020). Aave protocol whitepaper v1.0. Retrieved July 14, 2022, from https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf

Anson, M. (2021). Initial exchange offerings: The next evolution in cryptocurrencies. ***The Journal of Alternative Investments***, ***23***(4), 110–121. https://doi.org/10.3905/jai.2021.1.127

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51 % attack on blockchains: A mining behavior study. ***IEEE Access***, ***9***, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

APYSwap. (2021). NFTs tokenization explained. Retrieved July 14, 2022, from https://apys.medium.com/nfts-tokenization-explained-94a7f6f4fe99

Arnold, L., Brennecke, M., Camus, P., Fridgen, G., Guggenberger, T., Radszuwill, S., Rieger, A., Schweizer, A., & Urbach, N. (2019). Blockchain and initial coin offerings : Blockchain's implications for crowdfunding. ***Business transformation through blockchain. volume 1*** (pp. 233–272). Palgrave Macmillan. Retrieved July 14, 2022, from https://link.springer.com/chapter/10.1007/978-3-319-98911-2_8

Aspris, A., Foley, S., Svec, J., & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. ***International Review of Financial Analysis***, ***77***, 101845. https://doi.org/10.1016/j.irfa.2021.101845

Association of Chartered Certified Accountants. (2022). Holdings of cryptocurrencies. Retrieved July 14, 2022, from https://www.accaglobal.com/in/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-reporting/technical-articles/cryptocurrencies.html

Auffenberg, L. (2021). Delegated staking as crypto management –- BaFin assumes authorization requirement in certain constellations. Retrieved July 14, 2022, from https://fin-law.de/en/2021/06/21/delegated-staking-as-crypto-management-bafin-assumes-authorization-requirement-in-certain-constellations/

Auffenberg, L. (2022). DeFi business model crypto lending –- is it regulated? Retrieved July 14, 2022, from https://fin-law.de/en/2022/01/03/defi-business-model-crypto-lending-is-it-regulated/

Augur. (2018). The Augur white paper: A decentralized oracle and prediction market platform. Retrieved July 14, 2022, from https://medium.com/@AugurProject/the-augur-white-paper-a-decentralized-oracle-and-prediction-market-platform-ed8907401c48

Bachmann, N., Drasch, B., Miksch, M., & Schweizer, A. (2019). Dividing the ICO jungle : Extracting and evaluating design archetypes. ***Tagungsband Internationale Tagung Wirtschaftsinformatik*** (pp. 1723–1737). Universitätsverlag Siegen. https://aisel.aisnet.org/wi2019/track14/papers/1/

Ball, M. (2021). Framework for the metaverse. Retrieved July 14, 2022, from https://www.matthewball.vc/all/forwardtothemetaverseprimer

Bank for International Settlements. (2022). Central bank digital currencies: A new tool in the financial inclusion toolkit? Retrieved July 14, 2022, from https://www.bis.org/fsi/publ/insights41.htm

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). SoK: Consensus in the age of blockchains. ***Proceedings of the 1st ACM Conference on Advances in Financial Technologies***, 183–198. https://doi.org/10.1145/3318041.3355458

Barbereau, T., Sedlmeir, J., Smethurst, R., Fridgen, G., & Rieger, A. (2022a). Tokenization and regulatory compliance for art and collectibles markets. In M. Lacity & H. Treiblmaier (Eds.), ***Blockchains and the token economy: Studies in theory and practice***. Palgrave Macmillan.

Barbereau, T., Smethurst, R., Papageorgiou, O., Rieger, A., & Fridgen, G. (2022b). DeFi, not so decentralized: The measured distribution of voting rights. ***Proceedings of the 55th Hawaii International Conference on System Sciences***, 6043–6052. https://doi.org/10.24251/HICSS.2022.734

Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2022c). Decentralised finance's unregulated governance: Minority rule in the digital wild west. Retrieved July 14, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001891

Barthere, A., Choe, L., Baraki, B., Khoo, Y. L., Grushyn, P., Lim, X. Y., & Ho, J. (2022). On-chain forensics: Demystifying TerraUSD de-peg. Retrieved July 14, 2022, from https://www.nansen.ai/research/on-chain-forensics-demystifying-terrausd-de-peg

Bartoletti, M., Chiang, J. H.-y., & Lluch-Lafuente, A. (2021). A theory of automated market makers in DeFi. ***Coordination models and languages***. Springer. https://doi.org/10.1007/978-3-030-78142-2_11

Bebel, J., & Ojha, D. (2022). Ferveo: Threshold decryption for mempool privacy in BFT networks. Retrieved July 14, 2022, from https://eprint.iacr.org/2022/898

Bennett, S., Charbonneau, K., Leopold, R., Mezon, L., Paradine, C., Scilipoti, A., & Villmann, R. (2020). Blockchain and cryptoassets:

Insights from practice*. ***Accounting Perspectives***, *19*(4), 283–302. https://doi.org/10.1111/1911-3838.12238

Binance. (2021). As part of ongoing commitment to compliance, binance deploys ciphertrace traveler. Retrieved July 14, 2022, from https://www.binance.com/en/blog/all/as-part-of-ongoing-commitment-to-compliance-binance-deploys-ciphertrace-traveler-421499824684902268

Binance. (2022). What is staking? Retrieved July 14, 2022, from https://academy.binance.com/en/articles/what-is-staking

Biryukov, A., & Tikhomirov, S. (2019). Deanonymization and linkability of cryptocurrency transactions based on network analysis. ***European Symposium on Security and Privacy***, 172–184. https://doi.org/10.1109/EuroSP.2019.00022

Blockonomist. (2021). Ubisoft to launch the first energy-efficient and playable nfts platform. Retrieved July 14, 2022, from https://medium.com/geekculture/ubisoft-to-launch-the-first-energy-efficient-and-playable-nfts-platform-1b16d9e9a904

Blockworks. (2022a). 3AC files for bankruptcy as co-founders' location unknown. Retrieved July 14, 2022, from https://blockworks.co/3ac-files-for-bankruptcy-as-co-founders-location-unknown/

Blockworks. (2022b). Celsius clashes with lawyers over chapter 11 bankruptcy: Report. Retrieved July 14, 2022, from https://blockworks.co/celsius-clashes-with-lawyers-over-chapter-11-bankruptcy-report/

Bolotaeva, O. S., Stepanova, A. A., & Alekseeva, S. S. (2019). The legal nature of cryptocurrency. ***IOP Conference Series: Earth and Environmental Science***, *272*(3), 032166. https://doi.org/10.1088/1755-1315/272/3/032166

Brennecke, M., Guggenberger, T., Schellinger, B., & Urbach, N. (2022). The de-central bank in decentralized finance : A case study of MakerDAO. https://doi.org/10.24251/HICSS.2022.737

Buterin, V. (2014). A next generation smart contract & decentralized application platform. Retrieved July 14, 2022, from https://ethereum.org/en/whitepaper/

Buterin, V. (2021). Moving beyond coin voting governance. Retrieved July 14, 2022, from https://vitalik.ca/general/2021/08/16/voting3.html

Butijn, B.-J., Tamburri, D. A., & Heuvel, W.-J. v. d. (2020). Blockchains: A systematic multivocal literature review. ***ACM Computing Surveys***, *53*(3). https://doi.org/10.1145/3369052

Cadete de Matos, J., Fano, D., Lima, F., & Seneviratne, A. (2021). The role of financial markets. Retrieved July 14, 2022, from https://www.oecd-ilibrary.org/sites/9789264281288-5-en/index.html?itemId=/content/component/9789264281288-5-en

Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance – a multivocal approach. ***Applied Sciences***, *11*(16). https://doi.org/10.3390/app11167572

Cao, Y., Zou, C., & Cheng, X. (2021). Flashot: A snapshot of flash loan attack on DeFi ecosystem. Retrieved July 14, 2022, from https://arxiv.org/abs/2102.00626

Carbon Offset Guide. (2022). What is a carbon offset? Retrieved July 14, 2022, from https://www.offsetguide.org/understanding-carbon-offsets/what-is-a-carbon-offset/

Catalini, C., de Gortari, A., & Shah, N. (2021). Some simple economics of stablecoins. Retrieved July 14, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3985699

CBC/Radio-Canada. (2021). This man owns $321m in Bitcoin —- but he can't access it because he lost his password. Retrieved July 14, 2022, from https://www.cbc.ca/radio/asithappens/as-it-happens-friday-edition-1.5875363/this-man-owns-321m-in-bitcoin-but-he-can-t-access-it-because-he-lost-his-password-1.5875366

Chainalysis. (2021). The 2021 global crypto adoption index. Retrieved July 14, 2022, from https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

Chen, D. B., van der Beek, J., & Cloud, J. (2019). Hypothesis for a risk cost of carbon: Revising the externalities and ethics of climate change. In H. Doukas, A. Flamos, & J. Lieu (Eds.), ***Understanding risks and uncertainties in energy and climate policy*** (pp. 183–222). Springer. https://doi.org/10.1007/978-3-030-03152-7_8

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. ***Journal of Business Venturing Insights***, *13*, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151

Ciphertrace. (2021). Current trends in ransomware. Retrieved July 14, 2022, from https://4345106.fs1.hubspotusercontent-na1.net/hubfs/4345106/Content/Current%20Trends%20in%20Monero%20Usage%20and%20Ransomware_FINAL.pdf?utm_campaign=Research&utm_medium=email&_hsmi=210465645&utm_content=210465645

CoinBundle. (2018). What are airdrops? Retrieved July 14, 2022, from https://medium.com/coinbundle/what-are-airdrops-ab97b276b0d1

CoinDesk. (2022a). How crypto lender Celsius overheated. Retrieved July 14, 2022, from https://www.coindesk.com/business/2022/06/16/how-crypto-lender-celsius-overheated/

CoinDesk. (2022b). It's not just LUNA. terra's DeFi apps have hemorrhaged $28B. Retrieved July 14, 2022, from https://www.coindesk.com/markets/2022/05/20/its-not-just-luna-terras-defi-apps-have-hemmorhaged-28b/

CoinDesk. (2022c). Three arrows faces possible insolvency after unforeseen liquidations: Report. https://www.coindesk.com/markets/2022/06/15/three-arrows-faces-possible-insolvency-after-unforeseen-liquidations/

CoinGecko. (2020). Decentralized finance (DeFi). Retrieved July 14, 2022, from https://www.coingecko.com/en/glossary/decentralized-finance-defi

Coinmarketcap. (2022a). CeDeFi. Retrieved July 14, 2022, from https://coinmarketcap.com/alexandria/glossary/cedefi

Coinmarketcap. (2022b). Initial dex offering (IDO). Retrieved July 14, 2022, from https://coinmarketcap.com/alexandria/glossary/initial-dex-offering

Compound. (2020). Compound: The money market protocol. Retrieved July 14, 2022, from https://compound.finance/documents/Compound.Whitepaper.pdf

ConsenSys. (2020). DeFi report: An analysis of Ethereum's decentralized finance ecosystem in Q3 2020. Retrieved July 14, 2022, from https://f.hubspotusercontent10.net/hubfs/4795067/Codefi/consensys-q3-defi-report.pdf

Corbet, S., Goodell, J. W., Gunay, S., & Kaskaloglu, K. (2021). Are DeFi tokens a separate asset class from conventional cryptocurrencies? https://doi.org/10.2139/ssrn.3810599

Cousaert, S., Xu, J., & Matsui, T. (2022). SoK: Yield aggregators in DeFi. ***IEEE International Conference on Blockchain and Cryptocurrency***. https://doi.org/10.1109/ICBC54727.2022.9805523

Crown, S. (2018). The cryptoeconomics of seigniorage shares stablecoins. Retrieved July 14, 2022, from https://smithandcrown.com/research/the-cryptoeconomics-of-seigniorage-shares-stablecoins-basis-and-carbon/

Cryptopedia. (2022). What was the DAO? Retrieved July 14, 2022, from https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

Daian, P. (2016). Analysis of the DAO exploit. Retrieved July 14, 2022, from https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. ***IEEE Symposium on Security and Privacy***, 910–927. https://doi.org/10.1109/SP40000.2020.00040

Dedezade, E., Phillips, D., & Di Salvo, M. (2020). What is yield farming? beginner's guide. Retrieved July 14, 2022, from https://decrypt.co/resources/what-is-yield-farming-beginners-guide

DeFiLlama. (2022). Ethereum DeFi, total value locked 2019-2022. Retrieved July 14, 2022, from https://defillama.com/chain/Ethereum

Derviz, A. et al. (2021). Decentralised finance, its prospects and limits: Is blockchain interoperability the only obstacle? ***Occasional Publications-Chapters in Edited Volumes***, 13–17. https://www.cnb.cz/export/sites/cnb/en/monetary-policy/.galleries/geo/geo_2021/gev_2021_07_en.pdf

Dhillon, V., Metcalf, D., & Hooper, M. (2017). The DAO hacked. In V. Dhillon, D. Metcalf, & M. Hooper (Eds.), ***Blockchain enabled applications*** (pp. 67–78). Apress. https://doi.org/10.1007/978-1-4842-6534-5_6

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. ***IEEE Transactions on Knowledge and Data Engineering***, ***30***(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227

Djamali, A., Dossow, P., Hinterstocker, M., Schellinger, B., Sedlmeir, J., Völter, F., & Willburger, L. (2021). Asset logging in the energy sector: A scalable blockchain-based data platform. ***Energy Informatics***, ***4***(3), 1–20.

DKCrypto. (2021). Guide to yield farming & staking crypto assets. Retrieved July 14, 2022, from https://medium.com/geekculture/guide-to-yield-farming-staking-crypto-assets-ca2404097b90

Ernst & Young. (2019). Holdings of cryptocurrencies. Retrieved July 14, 2022, from https://www.ey.com/en_gl/ifrs-technical-resources/holdings-of-cryptocurrencies

Eskandari, S., Moosavi, M., & Clark, J. (2019). SoK: Transparent dishonesty: Front-running attacks on blockchain. In A. Bracciali, J. Clark, F. Pintore, P. Rønne, & M. Sala (Eds.), ***Financial cryptography and data security***. https://doi.org/10.1007/978-3-030-43725-1_13

Ethereum Foundation. (2021). Shard chains. Retrieved July 14, 2022, from https://ethereum.org/en/eth2/shard-chains/

European Union. (2019). Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending directive (EU) 2019/1937. Retrieved July 14, 2022, from https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets

Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. ***Nature***, ***563***(7732), 465–467. https://doi.org/10.1038/d41586-018-07449-z

Ferreira, A. (2021). FATF draft guidance targets DeFi with compliance. Retrieved July 14, 2022, from https://cointelegraph.com/news/fatf-draft-guidance-targets-defi-with-compliance

Feulner, S., Guggenberger, T., Stoetzer, J.-C., & Urbach, N. (2022a). Shedding light on the blockchain disintermediation mystery: A review and future research agenda.

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022b). Exploring the use of self-sovereign identity for event ticketing systems. ***Electronic Markets*, *forthcoming***.

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. Retrieved July 14, 2022, from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

Financial Action Task Force. (2022). Financial action task force - what do we do. Retrieved July 14, 2022, from https://www.fatf-gafi.org/about/whatwedo/

Financial Industry Regulatory Authority. (2013). 5270. front running of block transactions. Retrieved July 14, 2022, from https://www.finra.org/rules-guidance/rulebooks/finra-rules/5270

Financial Stability Board. (2022). Assessment of risks to financial stability from crypto-assets. Retrieved July 14, 2022, from https://www.fsb.org/wp-content/uploads/P160222.pdf

Fox, D. (2018). Cryptocurrencies in the common law of property. Retrieved July 14, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232501

Fridgen, G., Körner, M.-F., Sedlmeir, J., & Weibelzahl, M. (2019). (how) can blockchain contribute to the management of systemic risks in global supply networks?

Fridgen, G., Radszuwill, S., Urbach, N., & Utz, L. (2018a). Cross-organizational workflow management using blockchain technology – towards applicability, auditability, and automation. ***Proceedings of the 51st Hawaii International Conference on System Sciences***, 3507–3517. https://doi.org/10.24251/hicss.2018.444

Fridgen, G., Regner, F., Schweizer, A., & Urbach, N. (2018b). Don't slip on the initial coin offering (ico): A taxonomy for a blockchain-enabled form of crowdfunding. ***26th European Conference on Information Systems (ECIS)***.

FundiFinance. (2021). Using NFT contracts for fractional ownership. Retrieved July 14, 2022, from https://medium.com/coinmonks/using-nft-contracts-for-fractional-ownership-8d98b27db1b7

Gagliardoni, T. (2021). The poly network hack explained. Retrieved July 14, 2022, from https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/

German Federal Government. (2020). Effectively reducing CO_2 emissions. Retrieved July 14, 2022, from https://www.bundesregierung.de/breg-en/issues/climate-action/effectively-reducing-co2-1795850

German Federal Ministry of Finance. (2021). Einzelfragen zur ertragsteuerrechtlichen Behandlung von virtuellen Währungen und von sonstigen Token. Retrieved July 14, 2022, from https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Einkommensteuer/2022-05-09-einzelfragen-zur-ertragsteuerrechtlichen-behandlung-von-virtuellen-waehrungen-und-von-sonstigen-token.html

Glassnode. (2022). Glassnode studio: Crypto market data. Retrieved July 14, 2022, from https://studio.glassnode.com/

Gluchowski, A. (2019). Optimistic vs. ZK rollup: Deep dive. Retrieved July 14, 2022, from https://medium.com/matter-labs/optimistic-vs-zk-rollup-deep-dive-ea141e71e075

Goforth, C. R. (2018). U.s. law: Crypto is money, property, a commodity, and a security, all at the same time. ***Journal of Financial Transformation***. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3272975

Gola, C., & Sedlmeir, J. (2022). Addressing the sustainability of distributed ledger technology. ***Bank of Italy Occasional Paper***, (670). https://www.bancaditalia.it/pubblicazioni/qef/2022-0670/QEF_670_22.pdf?language_id=1

Government of the Principality of Liechtenstein. (2021). Law of 3 october 2019 on tokens and TT service providers (Token and TT Service Provider Act; TVTG). Retrieved July 14, 2022, from https://www.regierung.li/law#section14480

Griffin, J. M., & Shams, A. (2020). Is Bitcoin really untethered? ***The Journal of Finance***, *75*(4), 1913–1964. https://doi.org/10.1111/jofi.12903

Guazzo, G. (2020). Yield farming: What is it and how does it work? Retrieved July 14, 2022, from https://medium.com/coinmonks/yield-farming-what-is-it-and-how-does-it-work-452c7ce2c467

Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020a). The decentralized financial crisis. ***Crypto Valley Conference on Blockchain Technology***. https://doi.org/10.1109/CVCBT50464.2020.00005

Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020b). DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency. ***Proceedings of the 2nd ACM Conference on Advances in Financial Technologies***, 92–112. https://doi.org/10.1145/3419614.3423254

Guggenberger, T., Kuhn, M., & Schellinger, B. (2021a). Insured? Good! Designing a blockchain-based credit default insurance system for DeFi lending protocols. ***Proceedings of the 4th Middle East & North Africa Conference for Information System***. https://aisel.aisnet.org/menacis2021/8

Guggenberger, T., Schlatt, V., Schmid, J., & Urbach, N. (2021b). A structured overview of attacks on blockchain systems. ***Proceedings of the Pacific Asia Conference on Information Systems***. https://aisel.aisnet.org/pacis2021/100/

Gunther, T. (2021). The basic guide to cryptocurrency airdrops for beginners. Retrieved July 14, 2022, from https://medium.

com/altstable/the-basic-guide-to-cryptocurrency-airdrops-for-beginners-c5f899dfad1

Haihan, D., Jiaye, L., Sizheng, F., Zhonghao, L., Xiao, W., & Wei, C. (2021). Metaverse for social good: A university campus prototype. ***Proceedings of the 29th ACM International Conference on Multimedia***, 153–161. https://doi.org/10.1145/3474085.3479238

Hickey, L., & Harrigan, M. (2021). The bisq decentralised exchange: On the privacy cost of participation. ***Blockchain: Research and Applications***, 100029. https://doi.org/10.1016/j.bcra.2021.100029

Hoffman, D. (2020). Global public goods and the protocol sink thesis. Retrieved July 14, 2022, from https://newsletter.banklesshq.com/p/global-public-goods-and-the-protocol

Hughes, H. (2021). Designing effective regulation for blockchain-based markets. ***Journal of Corporation Law***, ***46***(4), 899–908. https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Hughes_Final_Web.pdf

Huili, W., Wenping, M., Fuyang, D., Haibin, Z., & Qianhong, W. (2021). Dynamic threshold ECDSA signature and application to asset custody in blockchain. ***Journal of Information Security and Applications***, ***61***, 102805. https://doi.org/10.1016/j.jisa.2021.102805

International Financial Reporting Standards Foundation. (2019). Holdings of cryptocurrencies. Retrieved July 14, 2022, from https://www.ifrs.org/projects/completed-projects/2019/holdings-of-cryptocurrencies/#published-documents

International Monetary Fund. (2020). Externalities: Prices do not capture all costs. Retrieved July 14, 2022, from https://www.imf.org/external/pubs/ft/fandd/basics/38-externalities.htm

Jensen, J. R., von Wachter, V., & Ross, O. (2021). How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions. Retrieved July 14, 2022, from https://arxiv.org/abs/2102.10096

Juliano, A. (2018). dYdX: A standard for decentralized margin trading and derivatives. Retrieved July 14, 2022, from https://whitepaper.dydx.exchange/

Kannengiesser, N., Lins, S., Sander, C., Winter, K., Frey, H., & Sunyaev, A. (2021). Challenges and common solutions in smart contract development. ***IEEE Transactions on Software Engineering***. https://doi.org/10.1109/tse.2021.3116808

Katona, T. (2021). Decentralized finance: The possibilities of a blockchain ”money lego” system. ***Financial and Economic Review***, ***20***(1), 74–102.

Khan, N., & Ahmad, T. (2022). DCarbonX decentralised application: Carbon market case study. https://doi.org/10.48550/arXiv.2203.09508

Kistner, K. J. (2019). How decentralized is DeFi? A framework for classifying lending protocols. Retrieved July 14, 2022, from https://medium.com/hackernoon/how-decentralized-is-defi-a-framework-for-classifying-lending-protocols-90981f2c007f

Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y., & Minca, A. (2020). Stablecoins 2.0: Economic foundations and risk-based models, 59–79. https://doi.org/10.1145/3419614.3423261

KlimaDAO. (2022). Klimadao: A catalyst for innovation within the voluntary carbon market. Retrieved July 14, 2022, from https://www.klimadao.finance/blog/klimadao-a-catalyst-for-innovation-within-the-voluntary-carbon-market

Krion, A. (2021). The DeFi boom is finally here, and blockchain gaming will reap the rewards. Retrieved July 14, 2022, from https://www.nasdaq.com/articles/the-defi-boom-is-finally-here-and-blockchain-gaming-will-reap-the-rewards-2021-02-22

Kugler, L. (2021). Non-fungible tokens and the future of art. ***Communications of the ACM***, ***64***(9), 19–20. https://doi.org/10.1145/3474355

Kursawe, K. (2021). Wendy grows up: More order fairness. ***International Conference on Financial Cryptography and Data Security***, 191–196. https://doi.org/10.1007/978-3-662-63958-0_17

Lau, Y. (2022). You'll soon be able to put your Metaverse avatar to work – and make actual money from it. Retrieved July 14, 2022, from https://fortune.com/2022/02/07/metaverse-avatar-work-make-money-nft/

Lipton, A., & Hardjono, T. (2021). Blockchain intra- and interoperability. ***Innovative technology at the interface of finance and operations***. Springer. https://doi.org/10.1007/978-3-030-81945-3_1

Lockl, J., & Stoetzer, J.-C. (2021). Trust-free banking missed the point: The effect of distrust in banks on the adoption of decentralized finance. ***Proceedings of the 29th European Conference on Informations Systems***. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1153/wi-1153.pdf

Maia, G., & Vieira dos Santos, J. (2021). MiCA and DeFi ('proposal for a regulation on market in crypto-assets' and 'decentralised finance'). https://doi.org/10.2139/ssrn.3875355

MakerDAO. (2020). How Dai helps meet the needs of the unbanked in America and beyond. Retrieved July 14, 2022, from https://blog.makerdao.com/how-dai-helps-meet-the-needs-of-the-unbanked-in-america-and-beyond/

Malwa, S. (2021). DeFi 'rug pull' scams pulled in $2.8b this year: Chainalysis. Retrieved July 14, 2022, from https://www.coindesk.com/markets/2021/12/17/defi-rug-pull-scams-pulled-in-28b-this-year-chainalysis/

Matsuo, S. (2020). Effectiveness of multi-stakeholder discussions for decentralized finance: A conference report of CoDeFi 2020. ***Financial cryptography and data security***. Springer. https://doi.org/10.1007/978-3-030-54455-3_16

McConaghy, M., McMullen, G., Parry, G., McConaghy, T., & Holtzman, D. (2017). Visibility and digital art: Blockchain as an ownership layer on the Internet. ***Strategic Change***, ***26***(5), 461–470. https://doi.org/10.1002/jsc.2146

Meegan, X., & Koens, T. (2021). Lessons learned from decentralised finance (DeFi). Retrieved July 14, 2022, from https://www.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2.0.pdf

Merkle Science. (2019). Hack track: Upbit cryptocurrency exchange. Retrieved July 14, 2022, from https://medium.com/merkle-science/hack-track-upbit-cryptocurrency-exchange-b1f17baa5a72

Mienert, B. (2021). How can a decentralized autonomous organization (DAO) be legally structured? Retrieved July 14, 2022, from https://lrz.legal/de/lrz/how-can-a-decentralized-autonomous-organization-dao-be-legally-structured

Miltenberger, O., Jospe, C., & Pittman, J. (2021). The good is never perfect: Why the current flaws of voluntary carbon markets are services, not barriers to successful climate change action. ***Frontiers in Climate***, ***3***. https://doi.org/10.3389/fclim.2021.686516

Monolith. (2021). Understanding DeFi: Layer 2 explained. Retrieved July 14, 2022, from https://medium.com/monolith/understanding-defi-layer-2-explained-6981ef6c8990

Munilla Garrido, G., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. (2021). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. Retrieved July 14, 2022, from https://arxiv.org/abs/2107.11905

Nägele, T. (2020). Liechtensteins tokens and tt service providers law. Retrieved July 14, 2022, from https://tokencontainermodel.com/liechtensteins-tokens-and-tt-service-providers-law-b23574d595f9

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. ***Decentralized Business Review***, 21260.

Newton, C. (2021). Mark in the Metaverse: Facebook's CEO on why the social network is becoming 'a Metaverse company'. Retrieved July 14, 2022, from https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2021). A survey on Metaverse: The state-of-the-art, technologies, applications, and challenges. Retrieved July 14, 2022, from https://arxiv.org/abs/2111.09673

Oliveira, L., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To token or not to token: Tools for understanding blockchain tokens. ***Proceedings of the 39th International Conference on Information Systems***. https://doi.org/10.5167/UZH-157908

Pourpouneh, M., Nielsen, K., & Ross, O. (2020). Automated market makers. Retrieved July 14, 2022, from https://www.econstor.eu/handle/10419/222424

PricewaterhouseCoopers. (2019). Cryptographic assets and related transactions: Accounting considerations under ifrs. Retrieved July 14, 2022, from https://www.pwc.com/gx/en/services/audit-assurance/publications/halo-solution-for-cryptocurrency.html

PricewaterhouseCoopers. (2021). Global crypto tax report. Retrieved July 14, 2022, from https://www.pwc.com/us/en/services/tax/library/releases-its-2021-global-crypto-tax-report.html

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021a). Cefi vs. DeFi – comparing centralized to decentralized finance. Retrieved July 14, 2022, from https://arxiv.org/abs/2106.08157

Qin, K., Zhou, L., & Gervais, A. (2021b). Quantifying blockchain extractable value: How dark is the forest? Retrieved July 14, 2022, from https://arxiv.org/abs/2101.05511

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2020). Attacking the DeFi ecosystem with flash loans for fun and profit. https://doi.org/10.48550/arXiv.2003.03810

Regner, F., Schweizer, A., & Urbach, N. (2019). Nfts in practice : Non-fungible tokens as core component of a blockchain-based event ticketing application. ***Proceedings of the 40th international conference on information systems***. https://aisel.aisnet.org/icis2019/blockchain_fintech/blockchain_fintech/1/

Reguerra, E. (2022). Solana network faces degraded performance for the second time this week. Retrieved July 14, 2022, from https://cointelegraph.com/news/solana-network-faces-degraded-performance-for-the-second-time-this-week

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU general data protection regulation. ***MIS Quarterly Executive***, ***18***(4). https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We need a broader debate on the sustainability of blockchain. ***Joule***, ***6***(6), 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013

Robinson, D., & Konstantopoulos, G. (2020). Ethereum is a dark forest. Retrieved July 14, 2022, from https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest

Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2022). Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit. ***International Journal of Information Management***, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476

Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. ***Information Processing & Management***, ***58***(4), 102584. https://doi.org/10.1016/j.ipm.2021.102584

Samaniego, M., Jamsrandorj, U., & Deters, R. (2016). Blockchain as a service for IoT. ***IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)***, 433–436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

Sams, R. (2014). A note on cryptocurrency stabilisation: Seigniorage shares. Retrieved July 14, 2022, from https://blog.bitmex.com/wp-content/uploads/2018/06/A-Note-on-Cryptocurrency-Stabilisation-Seigniorage-Shares.pdf

Schaffner, T. (2021). Scaling public blockchains. Retrieved July 14, 2022, from https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Schaer_DLTFintech/Lehre/Tobias_Schaffner_Masterthesis.pdf

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. ***Federal Reserve Bank of St. Louis Review***, (2), 153–174. https://doi.org/10.2139/ssrn.3571335

Schellinger, B. (2020). Optimization of special cryptocurrency portfolios. ***The Journal of Risk Finance***, ***21***(2), 127–157. https://doi.org/10.1108/JRF-11-2019-0221

Schellinger, B., Ante, L., & Bauers, S. B. (2022a). Blockchain use cases and concepts in sports: A systematic review. ***ECIS 2022 Research Papers. 49.*** https://aisel.aisnet.org/ecis2022_rp/49

Schellinger, B., Völter, F., Urbach, N., & Sedlmeir, J. (2022b). Yes, I do: Marrying blockchain applications with GDPR. ***Proceedings of the 55th Hawaii International Conference on System Sciences***, 4631–4640. https://doi.org/10.24251/HICSS.2022.563

Schirrmacher, N.-B., Jensen, J. R., & Avital, M. (2021). Token-centric work practices in fluid organizations: The cases of Yearn and MakerDAO. ***Proceedings of the 42nd International Conference on Information Systems***. https://aisel.aisnet.org/icis2021/is_future_work/is_future_work/17/

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (2016). Blockchain: Grundlagen, Anwendungen und Potenziale. Retrieved July 14, 2022, from https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf

Schrepel, T., & Buterin, V. (2020). Blockchain code as antitrust. ***Berkeley Technology Law Journal***. https://doi.org/10.2139/ssrn.3597399

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. ***Business & Information Systems Engineering***, ***62***(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. ***Electronic Markets***, 1–16. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Ross, P., Luckow, A., Lockl, J., Miehle, D., & Fridgen, G. (2021a). The DLPS: A framework for benchmarking blockchains. ***Proceedings of the 54th Hawaii International Conference on System Sciences***, 6855–6864. https://doi.org/10.24251/HICSS.2021.822

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021b). Digital identities and verifiable credentials. ***Business & Information Systems Engineering***, ***63***(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Sedlmeir, J., Völter, F., & Strüker, J. (2021c). The next stage of green electricity labeling: Using zero-knowledge proofs for blockchain-based certificates of origin and use. ***ACM SIGENERGY Energy Informatics Review***, ***1***(1), 20–31. https://doi.org/10.1145/3508467.3508470

Silberholz, J., & Di Wu, A. (2021). Measuring utility and speculation in blockchain tokens. https://doi.org/10.2139/ssrn.3915269

Solanews. (2021). Airdrops explained. Retrieved July 14, 2022, from https://solanews.substack.com/p/airdrops-explained?s=r

Song, J. (2017). Mt. Gox hack technical explanation. Retrieved July 14, 2022, from https://jimmysong.medium.com/mt-gox-hack-technical-explanation-37ea5549f715

Stevens, R. (2020). DeFi yield farming could threaten security of Ethereum 2.0. Retrieved August 7, 2022, from https://decrypt.co/46548/defi-yield-farming-threaten-security-ethereum

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., & Völter, F. (2021). Self-Sovereign Identity: Foundations, Applications, and Potentials of Portable Digital Identities. Retrieved July 14, 2022, from https://www.fim-rc.de/wp-content/uploads/2021/09/20210811-SSI-Whitepaper-English.pdf

Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing cryptocurrency exchange: Building up standard from huge failures. ***Financial cryptography and data security*** (pp. 254–270). Springer. https://doi.org/10.1007/978-3-030-54455-3_19

Sultanik, E., Remie, A., Manzano, F., Brunson, T., Moelius, S., Kilmer, E., Myers, M., Amir, T., & Schriner, S. (2022). Are blockchains decentralized? Unintended centralities in distributed ledgers. ***TrailOfBits***. Retrieved July 14, 2022, from https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. ***IEEE Network***, ***35***(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Fridgen, G., Spankowski, U., & Luckow, A. (2021). Token economy. ***Business & Information Systems Engineering***, ***63***(4), 457–478. https://doi.org/10.1007/s12599-021-00684-1

Synthetix. (2022). Synthetix litepaper. Retrieved July 14, 2022, from https://docs.synthetix.io/litepaper/

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Retrieved July 14, 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tabora, V. (2021). Money Legos and composability as DeFi building blocks. Retrieved July 14, 2022, from https://medium.com/the-capital/money-legos-and-composability-as-defi-building-blocks-efb1ad5e848e

Takanashi, Y. (2020). Future of finance. ***Financial cryptography and data security*** (pp. 242–253). Springer. https://doi.org/10.1007/978-3-030-54455-3_18

The World Bank. (2018). Financial inclusion on the rise, but gaps remain, global Findex database shows. ***World Bank Group***. Retrieved July 14, 2022, from https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows

The World Bank. (2021). The global Findex report 2021. Retrieved July 14, 2022, from https://www.worldbank.org/en/publication/globalfindex/Report

Tornaghi, C. (2022). Is crypto the path to financial inclusion in latin america? Retrieved July 14, 2022, from https://www.americasquarterly.org/article/is-crypto-the-path-to-financial-inclusion-in-latin-america/

U.S. Internal Revenue Service. (2022). Frequently asked questions on virtual currency transactions. Retrieved July 14, 2022, from https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions

U.S. Securities and Exchange Commission. (2017). Report of investigation pursuant to section 21(a) of the Securities Exchange Act of 1934: The DAO. Retrieved July 14, 2022, from https://www.sec.gov/litigation/investreport/34-81207.pdf

U.S. Securities and Exchange Commission. (2019). Leaders of CFTC, FinCEN, and SEC issue joint statement on activities involving digital assets. Retrieved July 14, 2022, from https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets

U.S. Securities and Exchange Commission. (2020). SEC charges Ripple and two executives with conducting USD 1.3 billion unregistered securities offering. Retrieved July 14, 2022, from https://www.sec.gov/news/press-release/2020-338

U.S. Securities and Exchange Commission. (2022). Crypto assets and cyber enforcement actions. Retrieved July 14, 2022, from https://www.sec.gov/spotlight/cybersecurity-enforcement-actions

Ushida, R., & Angel, J. (2021). Regulatory considerations on centralized aspects of DeFi managed by daos. ***Financial cryptography and data security. FC 2021 international workshops***. Springer. https://doi.org/10.1007/978-3-662-63958-0_2

Vermaak, W. (2022a). Crypto staking guide 2022. Retrieved July 14, 2022, from https://coinmarketcap.com/alexandria/article/crypto-staking-guide

Vermaak, W. (2022b). What are flash loan attacks? Retrieved July 14, 2022, from https://coinmarketcap.com/alexandria/article/what-are-flash-loan-attacks

Völter, F., Urbach, N., & Padget, J. (2021). Trusting the trust machine: Evaluating trust signals of blockchain applications. ***International Journal of Information Management***. https://doi.org/10.1016/j.ijinfomgt.2021.102429

Wachter, V., Jensen, J. R., & Ross, O. (2021). Measuring asset composability as a proxy for DeFi integration. ***Financial cryptography and data security. FC 2021 international workshops***. Springer. https://doi.org/10.1007/978-3-662-63958-0_9

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. ***IEEE Access***, ***7***, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized finance (DeFi). Retrieved July 14, 2022, from https://arxiv.org/abs/2101.08778

Whitaker, A., & Kräussl, R. (2020). Fractional equity, blockchain, and the future of creative work. ***Management Science***, ***66***(10), 4594–4611. https://doi.org/10.1287/mnsc.2020.3633

Wright, A. (2021). The rise of decentralized autonomous organizations: Opportunities and challenges. ***Stanford Journal of Blockchain Law & Policy***. Retrieved July

8, 2022, from https://stanford-jblp.pubpub.org/pub/rise-of-daos

Wright, A., & Meier, S. (2021). Analyzing FinCEN's proposed regulation relating to AML and KYC laws. ***Financial cryptography and data security. FC 2021 international workshops*** (pp. 54–62). Springer. https://doi.org/10.1007/978-3-662-63958-0_5

Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2021). SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. Retrieved July 14, 2022, from https://arxiv.org/abs/2103.12732

Yearn Finance. (2022a). What are yvaults? Retrieved July 14, 2022, from https://docs.yearn.finance/getting-started/products/yvaults/overview

Yearn Finance. (2022b). Yearn finance explained: What are vaults and strategies? Retrieved July 14, 2022, from https://blog.yearn.finance/articles/marco-worms/yearn-finance-explained-what-are-vaults-and-strategies

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. ***Journal of Financial Regulation***, ***6***(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Zhou, L., Qin, K., Cully, A., Livshits, B., & Gervais, A. (2021). On the just-in-time discovery of profit-generating transactions in DeFi protocols. ***IEEE Symposium on Security and Privacy***, 919–936. https://doi.org/10.1109/SP40001.2021.00113

Zhou, P. (2020). Understanding blockchain decentralization. Retrieved July 14, 2022, from https://medium.com/vechain-foundation/understanding-blockchain-decentralization-f8e753884977

Branch Business & Information Systems Engineering

The Branch Business & Information Systems Engineering of Fraunhofer FIT unites the research areas of Finance and Information Management in Augsburg and Bayreuth. Its special characteristics include expertise at the interface of financial management, information management, and information systems engineering as well as and the ability to combine methodical know-how at the highest scientific level with a customer-, target- and solution-oriented approach. Currently, our team consists of about 80 research assistants and more than 140 student assistants. Our research activities are thematically bundled in different research areas. This gives us extensive expertise in different areas of business informatics and enables us to transfer timely research results into practical solutions in applied research projects with numerous companies from different industries, thus creating long-term "win-win situations". Additionally, we are able to incorporate the knowledge gained into our numerous courses, so that we can provide our students with theoretically sound and practically relevant and up-to-date content. Our goal is to synergistically complement our range of topics with suitable research areas in the future as well.

Fraunhofer Blockchain Lab

Based on these overarching principles of the Branch Business & Information Systems Engineering, the Fraunhofer Blockchain Lab was founded, which is characterized by the interdisciplinary combination of economic, legal, and technical competencies. The Blockchain Lab designs, develops, and evaluates innovative solutions and is known for that far beyond national borders. Together with numerous partners from business and science, we work hard to comprehensively investigate the potential of blockchain technology and to make it accessible. At our location in Bayreuth, we have been supporting companies and public institutions in the context of applied research projects as well as in the development of individual and demand-oriented solutions in the field of blockchain technology since our foundation in 2016. Even though blockchain technology became known through its initial application as the basis of the cryptocurrency Bitcoin, it quickly became apparent that the actual potential of the blockchain extends much further. For example, in addition to business logic, mapped by so-called smart contracts, digital and self-managed identities are now also often implemented with the support of the blockchain.
In 2016, we were one of the first organizations in Germany to publish a white paper[15] in which we examined the fundamentals, applications and potential of blockchain technology as well and the role of intermediaries in various contexts. We have also received several awards for our work – including the Reallabore Innovation Prize from the German Federal Ministry for Economic Affairs and Energy and the eGovernment Prize for our project with the Federal Office for Migration and Refugees.

[15] See here.