BISE Student

https://bise-student.io

Bachelor's Thesis

A Multivocal Literature Review on Decentralized Finance

Current Knowledge and Open Research Agenda

Publication Date: 2023-10-31

Author
Marc Principato
University of Bayreuth
Bayreuth, Germany
marc.principato@fim-rc.de
0x2E1860728c1eb5622d4187efDF17E38b1f378621

Abstract

Since the emergence of blockchain technology from the world financial crisis as a decentral-ized peer-to-peer electronic cash system, financial activity on blockchains has evolved towards being more sophisticated and constituting a whole financial system. To date, this field of De-centralized Finance (DeFi) is novel and still little researched. Our work paves the way for a comprehensive understanding of DeFi by conducting a systematic multivocal literature re-view. We present a comprehensive definition and concept of DeFi. Furthermore, we summa-rize and analyze the current state of knowledge in the literature in a DeFi research framework and then identify urgent topics to be researched in DeFi. We conclude that DeFi is not ready for mainstream adoption as an alternative financial system yet, but it most certainly provides promising features that make research on it a worthwhile endeavor.

Keywords: Decentralized Finance, Blockchain, Fintech
Methods: Multivocal Literature Review

Submission Date: 2023-10-27
Submission Contract: 0x3CBB7b505807254A4b5A0E5f213b5E52707Cd31A

Faculty of Law, Business Management and Economics
Professorship Business Informatics & Digital Energy Management
Prof. Dr. Jens Strüker

Bachelor thesis

A Multivocal Literature Review on Decentralized Finance:

Current Knowledge and Open Research Agenda

Submitted by:
Marc Principato

Submission date:
13. Januar 2022

Supervisor:
Tobias Guggenberger
Benjamin Schellinger

German abstract

Seit dem Aufkommen der Blockchain-Technologie (als dezentralisiertes Peer-to-Peer-Electronic-Cash-System im Zuge der weltweiten Finanzkrise) haben sich die Finanzaktivitäten und -services auf Blockchains weiterentwickelt und entwickeln sich zu einem neuartigen Finanzsystem. Dieser Bereich der dezentralisierten Finanzen (DeFi) ist neuartig und noch wenig erforscht. Diese Arbeit ebnet den Weg für ein ganzheitliches Verständnis von DeFi, indem eine systematische und vielschichtige Literaturanalyse durchgeführt wird. Wir präsentieren eine umfassende Definition und ein Konzept von DeFi. Darüber hinaus wird der aktuelle Wissensstand in der Literatur zusammengefasst, analysiert und anschließend werden dringende Themen, die im Bereich DeFi erforscht werden müssen, identifiziert. Wir kommen zu dem Schluss, dass DeFi als alternatives Finanzsystem noch nicht bereit für die Mainstream-nutzung ist, aber vielversprechende Eigenschaften aufweist, die weitere Forschung und Entwicklung erforderlich machen.

English abstract

Since the emergence of blockchain technology from the world financial crisis as a decentralized peer-to-peer electronic cash system, financial activity on blockchains has evolved towards being more sophisticated and constituting a whole financial system. To date, this field of Decentralized Finance (DeFi) is novel and still little researched. Our work paves the way for a comprehensive understanding of DeFi by conducting a systematic multivocal literature review. We present a comprehensive definition and concept of DeFi. Furthermore, we summarize and analyze the current state of knowledge in the literature in a DeFi research framework and then identify urgent topics to be researched in DeFi. We conclude that DeFi is not ready for mainstream adoption as an alternative financial system yet, but it most certainly provides promising features that make research on it a worthwhile endeavor.

Table of contents

List of figures

List of tables

List of abbreviations

ABCD	Atomic bonded cross-chain debt
AEC	Anonymity-enhanced cryptocurrency
AL	Academic literature
AML	Anti-money-laundering
AMM	Automated market maker
CBDC	Central bank digital currency
CeFi	Centralized finance
CEX	Centralized exchange
CFMM	Constant function market maker
DeFi	Decentralized finance
DApp	Decentralized application
DAO	Decentralized autonomous organization
DEX	Decentralized exchange
ECDSA	Elliptic curve digital signature algorithm
E.g.	Exempli gratia
Et al.	Et alii
FinCEN	Financial crimes enforcement network
GL	Grey literature
ICO	Initial coin offering
IEO	Initial exchange offering
KYC	Know-your-customer
MEV	Miner extractable value
MLR	Systematic multivocal literature review
MSB	Money service business

P2P	Peer-to-peer
SEC	Securities and exchange commission
SLR	Systematic literature review
SSI	Self-sovereign identity
VTTP	Value token transfer protocol

1 Introduction

Decentralized finance (DeFi) is a new research field at the intersection of multiple disciplines (e.g.: Finance, Regulation, Technology) that emerged with the advent and evolution of blockchain technology and its application in the context of finance (Buterin 2013; Grigo et al. 2020). Through an interplay of decentralized infrastructure and financial applications, DeFi seeks to enable the functionality of a financial system in a digital and decentralized way (Schär 2021).

DeFi is seen to have significant disruptive potential regarding how financial activities will be conducted in the future (Chen and Bellavitis 2020; Grigo et al. 2020). While traditional financial activities often require trusted intermediaries (such as brokers or banks), DeFi aims to eliminate trusted authorities, disintermediate finance and create a trust-less environment using blockchains (Buterin 2016; Dai 1998; Schär 2021).

At the time of writing (December 2021), the total value locked in DeFi already corresponds to approximately $100B, meaning that this amount of value is currently supplied to the aforementioned financial applications on a blockchain.[1] However, DeFi still is a novel research field: initial works on DeFi were first published around 2019 and 2020 (Chen and Bellavitis 2019; Grigo et al. 2020).

To the best of our knowledge, there is yet no consistent definition and concept of DeFi across the literature (Katona 2021), and no work that systematically summarizes existing knowledge on DeFi. And as those amounts of value are put into a financial system of which little is known, severe problems like scams, frauds, and other illicit activities may arise quickly.[2]

Therefore, our goal is to bridge this gap by summarizing and analyzing existing knowledge to establish a common understanding of DeFi. We do this by conducting a multivocal literature review and aim to address the following research questions:

RQ1: What is DeFi, and how can it be defined?

RQ2: What kind of DeFi literature has been published, and how can they be systematized?

RQ3: What are the current research gaps in the field of DeFi?

---

[1] See: https://defipulse.com.

[2] See: 12B exploited in DeFi in 2021.

Based on the obtained body of knowledge, we draft an integrative and comprehensive definition and concept of DeFi to answer RQ1. Subsequently, the collected knowledge is presented in a DeFi research framework to illustrate the current state of DeFi and answer RQ2; this allows us to identify then pressing research areas in DeFi and provide a solid foundation for future research by answering RQ3.

The remainder of this work is organized as follows: chapter 2 elaborates on the blockchain and finance background. Chapter 3 describes the methodical procedure of the conducted multivocal literature review. In chapter 4, the findings of the conducted literature review are presented and discussed. Subsequently, we outline avenues for future research in chapter 5 and conclude this work in chapter 6.

2 Conceptual background

In the following, we will outline the fundamental concepts of the financial system and blockchain technology needed to understand the technology, philosophy, and aim of DeFi. We acknowledge that these concepts are highly complex with a large body of knowledge in their respective literature; thus, we only abstract the knowledge necessary for further understanding of this work.

2.1 Financial system

The financial system is a system that brings together the supply and demand side of capital (Barth and Brumbaugh 1997; Thakor 1996). It includes financial intermediaries, financial markets, and financial infrastructure (Deutsche Bundesbank 2019). ***Figure 1*** depicts an illustration of the financial system.

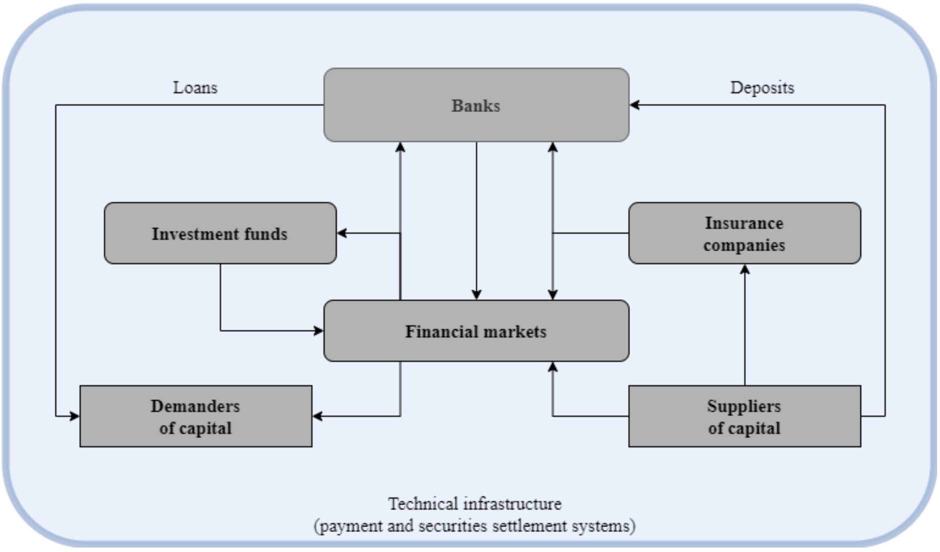


Figure 1: The financial system.
Source: Own illustration based on Deutsche Bundesbank (2021).

2.1.1 Money, banks, and value

Obtaining something that one cannot or does not want to produce was done initially by trading in a part of one's possession that is deemed equal worth for the object to be obtained (bartering). As bartering is not convenient, the concept of money as numeraire developed over time (Smith 1910). For this, money has to fulfill three essential functions: being means of exchange and payment, a unit of account, and a store of value (Deutsche Bundesbank 2019). Money can take on different forms like gold coins or banknotes that differ in the "value carrier material" of which they are made; thus, their intrinsic value can differ. So far, cash (outside/exogenous money) and book money (inside/endogenous money) have prevailed, often called fiat money. Fiat money lacks intrinsic value and can be reproduced at virtually no cost (Deutsche Bundesbank 2019). This is why a central authority that manages its supply, so that its value remains stable concerning asset prices, is needed (Deutsche Bundesbank 2019; Giles 2008; Jones and Rachlin 2008). This is called price stability management and a significant task of monetary policy.

While book money refers to the virtual money saved in bank accounts as data in a bank database, cash refers to tangible money, legal tender, and central bank money. Book money directly transfers into a claim of legal tender for non-banks. Lending and deposit-taking are the primary banking activities, and thus banks mainly intermediate between suppliers and demanders of capital and provide storage for money (Deutsche Bundesbank 2019). Due to the fractional reserve banking system, commercial banks can loan out more than the total deposited value available and thus create new book money. However, commercial banks are legally obliged to hold a certain amount of legal tender as a reserve that can only be created by the central bank to back their money creation process (McLeay et al. 2014). While this provides an ultimate limit to the money creation process of commercial banks, the central bank mainly influences the cost of borrowing (interest rate) for demanders of capital by setting the interest rates for legal tender money and thus indirectly controlling the book money creation by controlling the demand for loans (McLeay et al. 2014). The central bank and commercial banks form the banking and monetary system in which the central bank is tasked with achieving monetary policy goals, while commercial banks are often private institutions, intermediating and serving economic activity by managing money circulation on the money market (Deutsche Bundesbank 2019; Giles 2008).

2.1.2 Financial markets

While demanders, suppliers, banks, and brokers are participants of the financial system, financial markets are where they meet and can be classified based on why they meet (e.g.: different financial instruments). Major markets are the capital market (stocks/bonds), money market (credit/loans) and the derivatives market (swaps/futures/options/forwards) (Fabozzi 2008). The markets can be further divided into the primary market, on which the issuer of the financial instrument and investors trade, and the secondary market, on which investors trade existing instruments among each other. Financial markets are where the supply and demand side of funds meet - often through intermediaries - and trade towards a market equilibrium (Cadete de Matos et al. 2021). This carries major economic significance since those markets fulfill the function of price discovery and provide suppliers with investment opportunities while providing demanders of capital with options to source it, thus, reducing capital inefficiency, which means that money can be of use by supplying it to the financial system that would otherwise remain unspent and of no use for either demander or supplier (Barth and Brumbaugh 1997; Cadete de Matos et al. 2021; Lerner 1952).

2.1.3 Financial infrastructure and FinTech

The financial infrastructure determines how the financial instruments are transferred from supplier to demander and refers mainly to technological aspects of the financial system (Deutsche Bundesbank 2019). Over time financial technology (FinTech) companies have started to emerge as new intermediaries that are specialized in operating at the intersection of technology and the financial system, enhancing its infrastructure and services (e.g.: settlement services like VISA or PayPal) (Adrian and Shin 2010; Puschmann 2017; Schueffel 2017). For example, while it was once necessary to withdraw legal tender money in person to then conduct a transaction, technology has made it possible to realize the concept of electronic money (e.g.: credit/debit cards) and today’s convenient process of online banking over technical infrastructure (e.g.: VisaNet, SWIFT, TIPS) (ECB 1998). This contributed to the connection of financial intermediaries around the globe and the connection of national financial systems towards a global financial system (Adrian and Shin 2010).

The financial system primarily relies on the financial market intermediaries (e.g.: Brokers, money service businesses, commercial banks) for intermediation between suppliers and demanders of capital (Barth and Brumbaugh 1997). With the interconnectedness of financial systems and the emergence of securitization, where debts are wrapped to create a new asset that is tradeable, came a risk that spanned across a chain of intermediaries and ultimately contributed to the culmination of the subprime mortgage crisis of banks into the world financial crisis of 2007-2008 (Adrian and Shin 2010). Several adjustments to financial safeguard laws were made following that event, aiming to prevent such systemic risk. The financial infrastructure of CeFi includes the technology, laws, and regulations that form a framework in which participants of the financial system can act (Deutsche Bundesbank 2019; Thakor 1996).

2.2 Blockchain

The emergence of blockchains can be dated back to the publication of the bitcoin whitepaper in the cypherpunk mailing list by Satoshi Nakamoto (Nakamoto 2008). The technology incorporates previously existing technical and philosophical concepts. In the following, we will first cover the inception of blockchain and its concept and then cover the blockchain technology in itself.

2.2.1 Bitcoin and the emergence of blockchains

Bitcoin emerged from the world financial crisis as a peer-to-peer (P2P) electronic cash system with the goal to provide an alternative to the trust-based payment system in the form of a decentralized and trustless one (Nakamoto 2008). Bitcoin is inherently linked to distrust in central authorities such as banks and the state, which is famously represented in the statement of the genesis block of bitcoin: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”.[3] The cypherpunk movement subsequently seeks to replace the trust-based models with technology/cryptography and increase individuals' self-sovereignty (Hughes 1993; May 1994).

Since the digital book money can easily be copied and saving account data altered, a value transaction cannot be ensured to be irreversible and only spent once without a trusted central party; banks take central authority in this system to ensure that there is no such double-spending (Nakamoto 2008). This was seen to increase the cost of intermediation and the need to trust a central authority. The contribution of Bitcoin is the technological concept of a blockchain. A blockchain, in essence, is a decentralized database that stores all data in blocks, which are in turn chronologically linked to each other by hash functions (Butijn et al. 2019; Nofer et al. 2017). By chronologically linking the blocks that store the data, the blockchain is theoretically an irreversible database that can facilitate irreversible, non-replicable transactions of electronic money: a solution to the double-spending problem (Dai 1998; Nakamoto 2008).

[3] See: Bitcoin genesis block.

2.2.2 Blockchain technology

Figure 2 depicts a simplified structure of a blockchain.

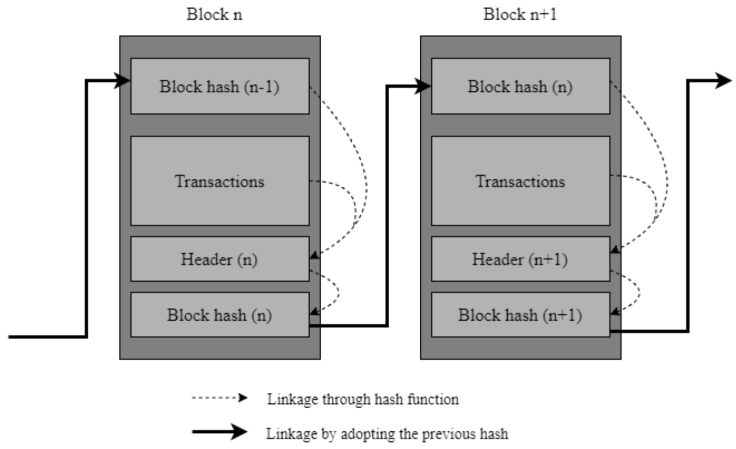


Figure 2: Simplified structure of a blockchain.
Source: Own illustration based on Nakamoto (2008).

Each participant (= node) in the blockchain network has an identical copy of the blockchain (= ledger) in the initial position. If new transactions are made, they are signed by asymmetric encryption and sent to all nodes in the P2P network[4]. Nodes accumulate and store raw transactions that are yet not added to the blockchain in a memory pool. A subset of nodes, called validators or miners, batches the raw transactions and their hash[5] in a block (Nakamoto 2008). The transaction hashes get combined and hashed in a Merkle tree, which results in a "hash of hashes" that results from and includes all individual transaction hashes and is called merkle root (Merkle 1988; Nakamoto 2008). The merkle root and the previous block hash will then be used as inputs to a hash function, which will output the header of the current block. This process concatenates the current block with the previous block by a cryptographic hash function (Nakamoto 2008). A cryptographic hash function is collision-resistant, which means that it is almost impossible to have different input values for the same hash value (Rogaway and Shrimpton 2004). A consensus mechanism now decides who is authorized to create the new block and what requirements the block hash must fulfill (Butijn et al. 2019). The creation is completed by producing the block hash from the header, using a hash function. With the requirements for the block hash, the difficulty of block creation can be artificially influenced to ensure security in

[4] A P2P network is a network in which each node acts as a server and client simultaneously.

[5] A cryptographic hash function is an irreversible mathematical function that maps input data of any length to a hash value of a fixed length. The outcome is called a hash.

the P2P network (Butijn et al. 2019; Nofer et al. 2017). The block is sent to all nodes via the P2P network and is checked against the requirements. If these are met, and the nodes validate the block hash, there is consensus, and the block is added to every individual ledger and thus the blockchain (Nakamoto 2008). The blockchain is now in a new starting position.

2.2.3 Blockchain properties

While traditional databases act as a black box to clients and require users' trust (e.g.: a bank’s database), blockchains are **transparent** by publishing transactions in the P2P network (Tai et al. 2017).

As a database, the blockchain does not tangibly exist but rather is a concept of consensus decision-making over the one single truth (deterministic system state) in a network of **pseudonymous** participants that might act maliciously or have deviant system states (Nakamoto 2008). This is often referred to as Byzantine fault tolerance (Castro et al. 1999).

A blockchain is a database without central accumulation of data because the data is stored on distributed ledgers and structured in blocks (contrary to regular databases that use file servers as storage and tables as structurization), meaning that the data exists on every single full node’s data storage (ledger) in the P2P network of the blockchain and is thus **distributed** (Nakamoto 2008).

Every added block alters the state of the blockchain (state transition). When executed on every ledger, this state transition should lead to the same result (same new state) because of the consensus mechanism (Buterin 2013; Nakamoto 2008). Hence a blockchain aims to be a **deterministic** database (Tai et al. 2017). Because of determinism, the blockchain cannot query data from outside (on-chaining) by itself. For some applications, the blockchain thus needs data feeds (oracles) operated by agents that intermediate between the deterministic “blockchain world” and the non-deterministic outside by on-chaining information. As it is not possible to check for the veracity of this information automatically, the blockchain relies on these agents to perform honestly. This is often referred to as the oracle problem (Caldarelli 2020).

The power to send, process, and validate transactions is distributed among the nodes. Thus the blockchain is also **decentralized** (Nakamoto 2008). Transactions require and are signed by a private key, making transactions **tamper-resistant** (Tai et al. 2017). Further, the blockchain is theoretically **irreversible/immutable** because of its block creation and block validation process. If data in an old block is to be altered, a new block is created because any other variation of data results in another block hash, which in turn has as a consequence that every following block is a new one and needs to be calculated and accepted anew. As long as the majority of participants act honestly, it is thus not possible to change the data history. If 51% of validator power is acquired, often referred to like 51% attack, such manipulation can become feasible (Nakamoto 2008).

Transactions grouped in a block are **atomic** (Tai et al. 2017). Atomicity of a database refers to an indivisible database operation, meaning that it did not exist in the previous state but appears fully executed in the next state (Buterin 2013). A transaction is either executed or is not; it is not possible for it to only be partially executed.

The aforementioned properties are crucial to enabling a trustless and decentralized P2P payment and value transfer system (Buterin 2013; Dai 1998; Nakamoto 2008). Compared to other databases, blockchains compromise scalability for achieving these properties; the blockchain network has a **limited throughput** (scalability), it could become congested, which is often referred to as the scalability problem (Butijn et al. 2019; Chauhan et al. 2018). A standard solution to that is assigning a price (gas fee) to every operation on it, which value gets “burned” in the course of the execution (Buterin 2013; Tai et al. 2017). The higher the computational work in the network, the higher the needed amount of gas for an operation.

2.3 Financial system on blockchain(s): DeFi

It is possible to store protocols and execute code on a blockchain. This is done by storing the code and executing it on the individual nodes; hence these protocols are executed in a decentralized way (Buterin 2013). Often referred to as smart contracts, these protocols can be executed by initiating a transaction to the smart contract's address (Buterin 2013; Szabo 1994). The first blockchain to incorporate them was Ethereum (Buterin 2013, 2016).

While Bitcoin is mainly designed for payments, Ethereum, with its integration of smart contracts, enabled more sophisticated financial services (Grigo et al. 2020; Tapscott and Tapscott 2017; Varma 2019). Currently, no clear definition of decentralized finance exists (Cao et al. 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021; Ushida and Angel 2021). However, first works regarding its concept and technical implementation do exist. ***Figure 3*** illustrates a concept of DeFi based on different layers.

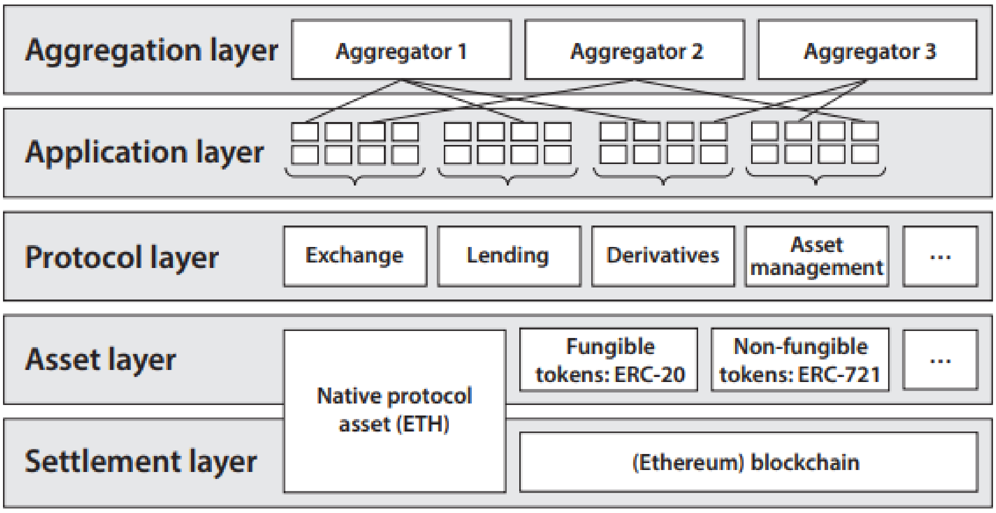


Figure 3: The DeFi stack.

Source: Schär (2021).

DeFi uses blockchain as infrastructure to enable financial services based on smart contracts and facilitate value transfers and payments via the blockchain as a settlement tool (Buterin 2016; Grigo et al. 2020; Werner et al. 2021). Smart contracts provide standards that can be used as building blocks for DeFi applications (Buterin 2013, 2016; Werner et al. 2021). Individual DeFi applications can be further aggregated to service aggregators that provide users financial services spanning over multiple individual applications (Grigo et al. 2020; Schär 2021). Smart contracts/blockchain protocols provide a back-end for the DeFi applications, which a web-based front-end can often access. The native assets herby originate from the blockchain itself, while non-native assets are often called tokens and refer to protocol assets that are standardized so that they can be transferred and used between different protocols (Buterin 2013; Schär 2021). DeFi protocols and assets are thus highly interoperable, earning it the name "Money Lego" (Grigo et al. 2020).

While Bitcoin is mainly a concept for providing an alternative and decentralized value and payment system, based on that infrastructure DeFi also aims to provide sophisticated decentralized and trustless financial services; essentially creating an alternative financial system on blockchain(s) (Chen and Bellavitis 2020; Grigo et al. 2020).

3 Research methodology

3.1 Aim and research questions

As pooled knowledge on DeFi is scarce, our research objective is to structure existing knowledge on DeFi and identify new research avenues. Subsequently, we aim to address the following research questions:

RQ1: What is DeFi, and how can it be defined?

RQ2: What kind of DeFi literature has been published, and how can they be systematized?

RQ3: What are the current research gaps in the field of DeFi?

The first research question aims to give an integrative definition and overview of the concept of DeFi. RQ2 aims to systematically categorize and summarize the published literature and body of knowledge in the DeFi field. Subsequently. Lastly, RQ3 seeks to present research gaps in DeFi that can be addressed through future research. The research questions are intentionally posed in a very broad manner to examine the topic of DeFi as a whole.

It has been argued extensively that excluding grey literature (GL) and only focusing on academic literature (AL)[6] in software engineering can have several negative impacts on the quality of literature reviews (Garousi et al. 2016; Kamei et al. 2021). Furthermore, the inclusion of GL brings several additional advantages (e.g.: preventing publication bias and pooling knowledge of academics and practitioners) (Buck et al. 2021; Garousi et al. 2019) that we would like to use to meet our research objective. Consequently, we chose to conduct a systematic multivocal literature review (MLR) following the approach of Garousi et al. (2019),[7] which supplements the well-established guidelines for systematic literature reviews (SLR) of Kitchenham and Charters (2007) with a process for including GL, hence turning it into guidelines for MLRs.

[6] For further explanations and differentiations of AL and GL we refer the interested reader to Garousi et al. (2016, 2019).

[7] Additionally, Garousi et al. (2019) provide a checklist on when conducting a MLR can yield benefits; their conditions listed are satisfied for our work.

3.2 Data sources and search strategy

The MLR search process can be subdivided into identifying the relevant AL and GL. First, we conduct the SLR search process for AL following the guidelines of Kitchenham and Charters (2007). Second, we conduct the GL search process following the guidelines of Garousi et al. (2019). We, therefore, obtain a predefined process to identify all relevant AL and GL for our research objective. A well-established predefined process/protocol additionally provides the benefit of reducing researcher bias. ***Figure 4*** illustrates our approach.

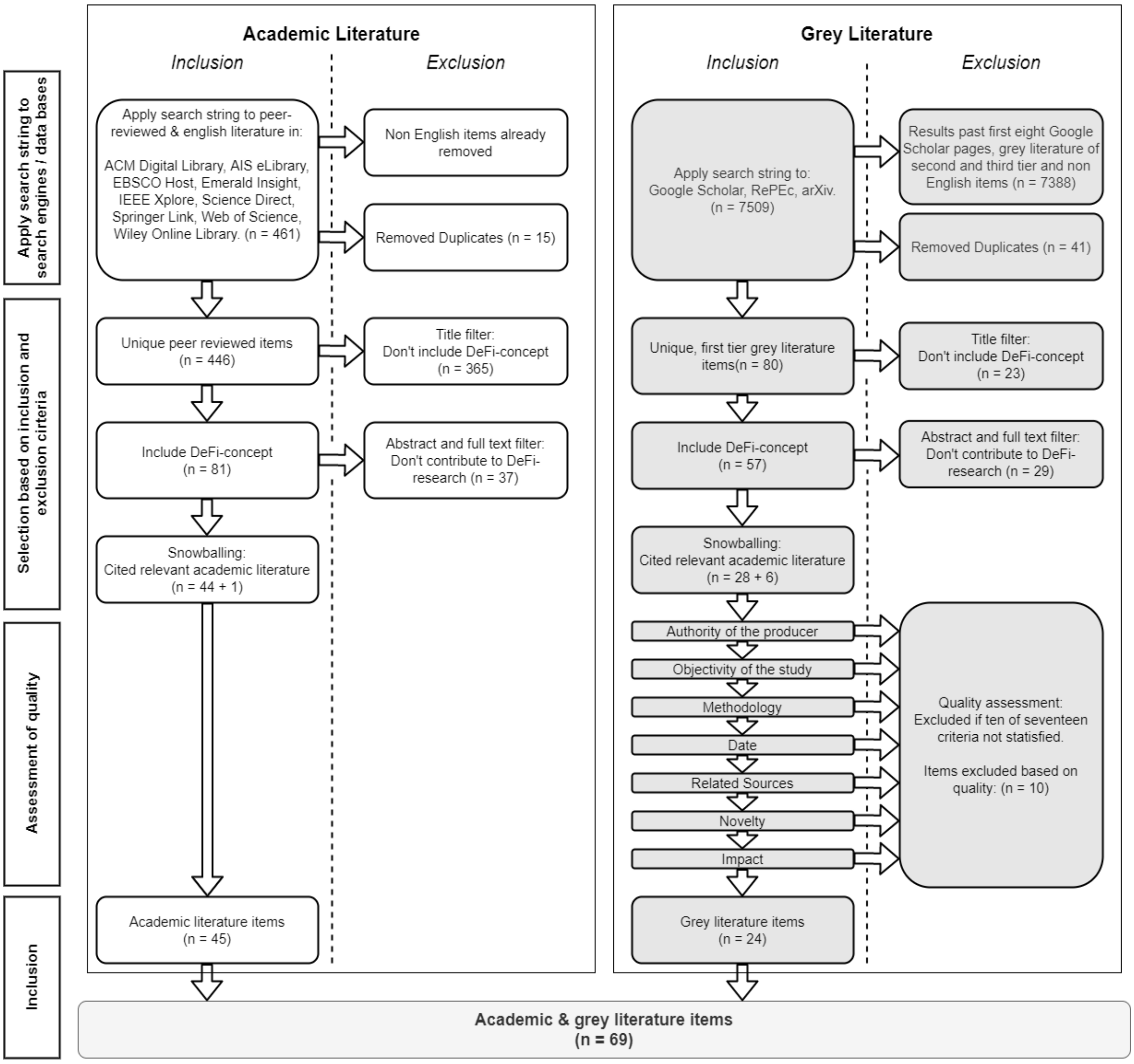


Figure 4: Illustration of sample selection and elimination process for this work.
Source: Own illustration based on Butjin et al. (2020) and Buck et al. (2020).

3.2.1 Identifying relevant academic literature

Following Kitchenham and Charters' (2007) approach, we start by developing a search string deemed appropriate for our research objective. We start with an initial search on Google Scholar with the terms "Decentralized Finance" and "DeFi" to obtain a broad overview and determine relevant related terms for our search string. Every new obtained term and variation of a search string is tested in terms of quality and inclusion rate.[8] The resulting search string is as follows:

(("Decentralized Finance" OR "Decentralised Finance" OR "DeFi" OR "Open Finance") AND ("Distributed Ledger" OR "DLT" OR "Blockchain"))

The search string is subsequently applied to nine well-established and reputable databases for AL: ACM Digital Library, AIS eLibrary, EBSCO Host, Emerald Insight, IEEE Xplore, Science Direct, Springer Link, Web of Science, and Wiley Online Library. The search (conducted in December 2021) initially yielded 461 AL items.

To further refine the obtained AL, we define inclusion and exclusion criteria. Items (1) with available full text, (2) published in peer-reviewed journals or conferences, and (3) that explore the concept of DeFi are included. We exclude AL items that (1) only briefly mention the concept of DeFi without contributing to the state of knowledge and (2) are not written in English (We used filter options in the respective databases to ensure that obtained items are already in English). The criteria are applied by title, abstract and full-text screening.

Finally, we perform forward and backward snowballing to include further relevant literature that might not be included in the subset of AL literature obtained through applying the search string (Webster and Watson 2002). The aforementioned inclusion and exclusion criteria were applied to evaluate the newly obtained set of AL. We identified 1 additional item. The SLR search process resulted in a total of 45 relevant AL items.

[8] For detailed insight into our methodology, please see: Excel-file.

3.2.2 Identifying relevant grey literature

The process of identifying relevant grey literature is guided by the approach of Garousi et al. (2019). Since there are three tiers of GL with different outlet control and credibility (Garousi et al. 2019), we opted to only include GL of the first tier for quality reasons. Again, we start by finding an appropriate search string. We used the gained insights from the AL search process and found the same search string to be suitable for GL databases:

(("Decentralized Finance" OR "Decentralised Finance" OR "DeFi" OR "Open Finance") AND ("Distributed Ledger" OR "DLT" OR "Blockchain"))

We applied this search string to Google Scholar, RePEc, and arXiv, which are databases deemed appropriate for a search of first-tier GL (Garousi et al. 2019). The initial search (conducted in December 2021) yielded 7509 Gl items. Following the guidelines, we established a stopping rule for the GL search. We opted to adopt the sophisticated stopping criteria of Butijn et al. (2019): we include the first eight pages of each database and incrementally evaluate the items on the following sites based on inclusion and exclusion criteria; if <50% of the page were not relevant, the search was stopped there. Only the search in Google Scholar yielded more than eight pages of literature.

Relevance is determined based on the inclusion and exclusion criteria for GL. GL items are included if (1) the GL item can be assigned to the first tier of GL by (Garousi et al. 2019), (2) the full text is available, and (3) it explores the concept of DeFi. GL items are excluded if (1) they only mention the concept of DeFi without contributing to the state of knowledge, and (2) they are not written in English.

We again perform forward and backward snowballing and identify 6 additional GL items. Since GL does not follow a peer-reviewed publishing process, the quality of items may vary. The guidelines for MLR hence provide a procedure with different criteria for assessing the individual quality of each item (Garousi et al. 2019), which we adopt for this task. Items that do not satisfy ten of seventeen criteria are excluded. Appendix A contains an overview of the GL quality criteria.

In total, after the assessment, 24 relevant GL items remained. See Appendix B for an overview of all identified articles from the MLR search process and their respective IDs.

4 Findings and discussion

4.1 Descriptive overview

Figure 5 depicts the distribution of identified relevant literature items per year.

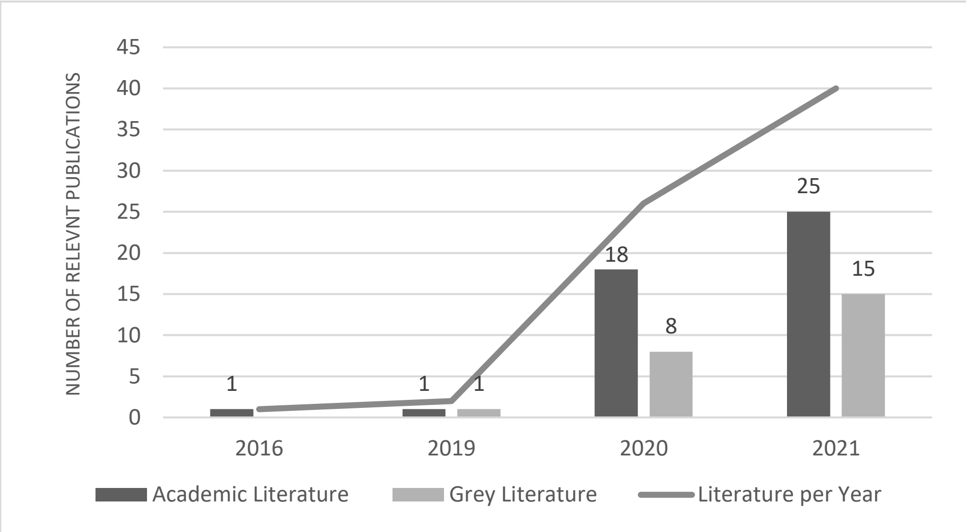


Figure 5: Distribution of AL and Gl over time.
Source: Own illustration.

Considering the publication dates of the items, our results match with previous findings and statements that DeFi is currently gaining much attention in research (Grigo et al. 2020; Schär 2021). From 2016 to 2019, DeFi only gained little attention from scholars and practitioners. In 2020, there is a significant increase in AL (+18) and a medium increase in GL (+8). However, GL contributions per year almost doubled from 2020 to 2021, while AL only saw a medium increase.

The sources of the literature items are heterogenous (see ***Figure 8***). While most of the AL are conference papers (n=31) and the rest are journal articles (n=14), the entirety of GL is almost equally distributed between eprints, preprints, technical reports, whitepapers, and working papers.

A first analysis of the GL quality assessment shows that the GL items generally have a low rating of impact (6%) while having a relatively high measure of novelty (69%), suggesting that either GL items often do not get considered in DeFi research despite contributing to the body of knowledge or are too recently published to be included in already published work. Additionally, GL items are generally highly rated in terms of date (94%), related sources (91%), and authority of the producer (76%), while being moderately rated in terms of objectivity of the source (58%) and methodology (50%). These results generally align with our expectations, considering that GL of the first tier has the highest quality, and no quality category except impact is rated < 50%. See Appendix A for the analysis of the GL assessment process.

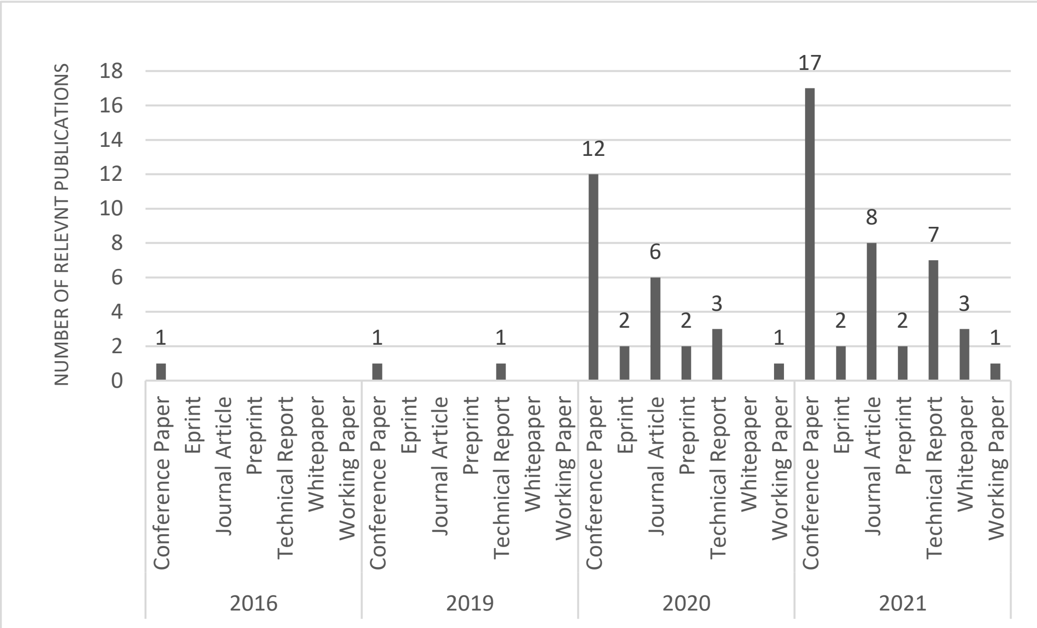


Figure 6: Distribution of publication venues per year.
Source: Own illustration.

4.2 DeFi-ning DeFi

While there exist different definitions of DeFi and a first conceptual framework, we want to move from individual definitions and frameworks towards a meta-definition and a comprehensive conceptual framework of DeFi by using the previous pooled knowledge from the entire body of DeFi literature.

4.2.1 Conceptual framework

To the best of our knowledge, the work of Schär (2021) is the first and only work that proposes a conceptional framework of DeFi. This framework subparts DeFi into different layers and considers them isolated from each other. Based on the body of knowledge in the identified literature on DeFi, we argue that DeFi cannot be divided into layers isolated from each other in practice. ***Figure 5*** illustrates our proposed DeFi framework.

One has to differentiate in a DeFi system between the infrastructural service that the blockchain provides for facilitating trustless payments and the functions that the protocols on it provide.

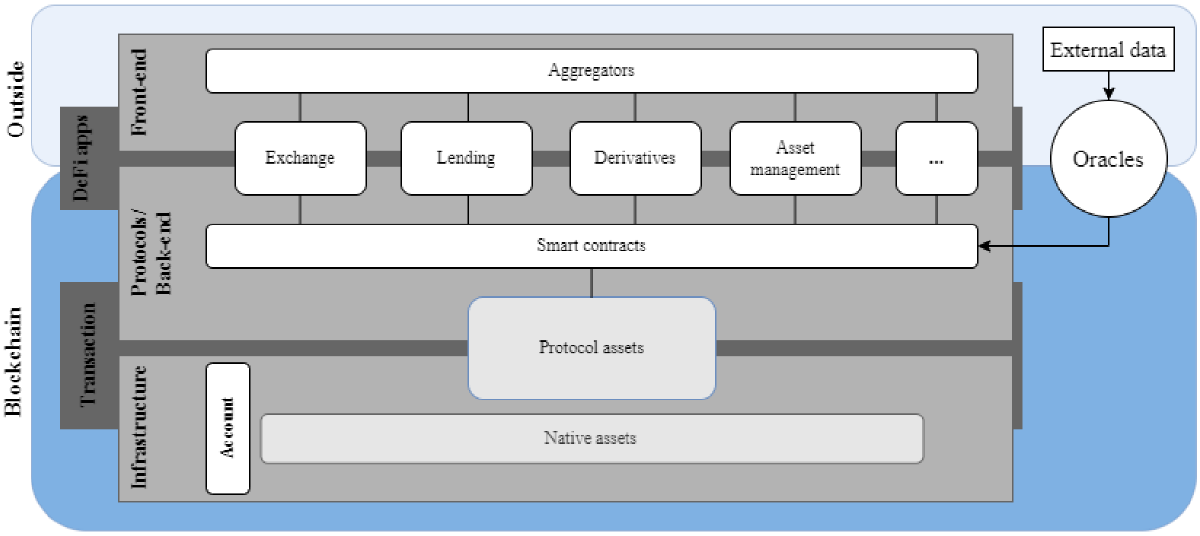


Figure 7: Conceptual DeFi framework.
Source: Own illustration.

On an infrastructural level, the blockchain stores (1) "accounts" in which the current balance of native and non-native assets is stored and (2) protocol code, while (3) enabling the mechanism explained in 2.2.3 (transactions), where the native asset is used as gas. The native asset originates from the blockchain code, and thus the infrastructure enables a "native monetary/value system".

DeFi applications are a subset of decentralized applications (Dapps) with financial use-cases and build a bridge between the "blockchain world" and the outside because they can be accessed by a browser-based front-end but source their data from smart contracts and execute its code on the blockchain. Neither back-end nor front-end are DeFi apps but the combination of both (see {DeFi Applications} in chapter 4.3). Non-native assets (tokens) originate from those protocols, and thus the protocol code enables a "non-native monetary system". The infrastructural service of the blockchain and its DeFi apps are connected by respective protocols and are highly intertwined (see: {Blockchain Infrastructure};{DeFi Applications} in chapter 4.3).

From a conceptional view, we argue that a DeFi system and the traditional financial systems are similar: the blockchain and stored protocol codes provide the infrastructure while DeFi applications and protocols enable financial markets (e.g.: automated market makers). One can thus split DeFi into an infrastructural blockchain layer and a DeFi application layer (as we did for adapting the research framework in chapter 4.3). Schär (2021) also acknowledges this differentiation in DeFi. However, these layers do not exist isolated from each other, are intertwined, and have dependencies. We acknowledge that the framework of Schär (2021) has advantages that stem from being simplistic and providing a precise categorization of DeFi parts into layers but may be misleading for future research on individual DeFi parts since they do not exist in isolation but in complex interplay.

4.2.2 Definition

Out of the 69 identified literature items, only 30 contained a clear definition of DeFi. Most of these definitions comprise a mixture of finance, technology, and goals. Current definitions are not consistent; while, for example, Qin, Zhou and Gervais (2021) refer DeFi to only as finance-focused applications on blockchains, Corbet et al. (2021) refer only to the financial services/products, and Katona (2021) refers to DeFi as an eco-system, including both. See ***Table 1*** for a summary of the definition analysis.

[#]	Finance				Technology			Goals				
	Sevices / Instruments	Markets	Infrastructure	Financial system	DLT / Blockchain	Smart contracts / protocols	DeFi Apps	Decentralization	Open-access	Automatization	New services	Composability
1				x	x	x						
46	x			x	x	x		x	x			
47	x							x				
51	x				x	x						
7	x			x	x			x	x			
9	x							x				
52	x			x	x	x	x		x			x
53	x				x	x		x	x			x
10			x		x	x	x	x	x			x
11		x				x						
55				x	x			x				
12	x					x						
56	x				x	x						
13				x	x			x				
14	x				x						x	
58				x	x		x		x			
59					x		x	x				
60					x		x	x	x			x
61	x				x	x		x				
62	x				x	x			x			
64	x			x	x	x	x	x	x			x
30					x	x	x	x				
65				x		x	x	x		x		
34				x			x	x				
42					x	x		x	x			
43				x	x	x		x				
67				x	x			x				
44	x				x	x	x	x	x			
68	x							x				
69			x	x	x			x	x	x		x

Table 1: Analysis of definitions.
Source: Own illustration.

We combine these definitions with regards to the body of knowledge identified by our MLR:

Decentralized Finance (DeFi) refers to financial activities in a decentralized financial system (DeFi system) that makes use of public blockchains as financial infrastructure, on top of which DeFi applications enable financial markets and services (= intermediation of financial instruments on those markets). This DeFi system aims to facilitate, decentralize, distribute, and automate the process of exchanging funds (by financial instruments over respective financial markets) between demanders and suppliers of funds.

DeFi is thus an abstract term that cannot be assigned to a single blockchain but rather generally to activities on DeFi platforms with financial system functionalities (e.g.: "DeFi <u>on</u> Ethereum"). A borderline case where this definition proves itself is Bitcoin. Whether Bitcoin belongs to

DeFi is not addressed in the identified literature. What is special about this question is that Bitcoin does not offer smart contract functionality but provides a financial infrastructure (payment/deposit services and a native value system) (Nakamoto 2008). We argue that Bitcoin thus belongs to DeFi like a monetary/value system, and the payment and deposit system/ functionality belongs to a financial system (see chapter 2.1). It is not a financial system itself but a substantial part of it. Since our definition is functionality-focused, activity on Bitcoin is included in a broader sense of DeFi, while activity on Etherum, for example, is DeFi in the narrower sense since it has the infrastructure plus sophisticated DeFi Apps (Buterin 2013).

4.3 Classification framework: knowledge synthesis

To meet our RQ2 and RQ3 research objective, it is necessary to systematically structure the literature from the MLR search process. Thus we adopt and modify the blockchain research classification framework of Risius and Spohrer (2017). We believe that their framework can be used as a classification foundation in the context of DeFi research, considering that DeFi is reliant on blockchain(s) as underlying infrastructure. Buck et al. (2021) argue that the blockchain framework is applicable in the context of zero-trust because of the similarities between both concepts and the research in each, respectively. We argue that in the context of DeFi, this applies even more so because both concepts and thus their research are intertwined (See chapter 2.3).

The classification framework addresses two dimensions: (a) activities and (b) level of analysis (Risius and Spohrer 2017). However, we want to take the intertwinement of DeFi and blockchain research into account. Hence, we opted to split the {Platforms} level into two separate ones: {DeFi Applications} and {Blockchain Infrastructure}. Furthermore, we changed {Firms and industries} to {Financial Industry} since blockchain technology can be used in different industries, but DeFi is an application of blockchain in the financial sector (See chapter 2.3). The level {Intermediaries} was then removed because the relevant financial intermediary services are now included in the levels of analysis {DeFi Applications} and {Financial Industry}. ***Table 2*** presents our adapted framework with IDs of the categorized literature items, where black IDs refer to AL and blue IDs to GL. For the framework with literature references, please see Appendix C.

(a) Activities address the actions performed in DeFi research; they are divided into three groups. {Design & Features} refers to the implementation and design of concepts as well as their features. {Measurement & Value} addresses benefits and disadvantages, added value, and conduct evaluations, and {Management & Organization} deals with governance, use, and overall organization.

(b) Level of analysis refers to the levels on which the respective activity is carried out; it is divided into four groups. {Users & Society} focuses on the group of users and the general public. {DeFi Applications} concerns the respective smart contracts, protocols, and apps on the blockchain which are necessary for DeFi. {Blockchain Infrastructure} targets the underlying blockchain, and {Financial Industry} focuses on the traditional financial industry with established firms and institutions.

The resulting categories from the combination of the two dimensions have proven to be extremely useful in the context of our work. The categories obtained allow us to examine DeFi from different perspectives abstracted from the identified literature, and thus the framework represents a valuable tool for achieving our research objectives.

It is important to note that the resulting categories are non-exclusive, meaning that a literature item can be assigned to multiple categories (Risius and Spohrer 2017).

Level of analysis \ Activities	Design & Features	Measurement & Value	Management & Organization
Users & Society	[5], [8], [45], [66], [67], [68]	[4], [5], [10], [51], [52], [55], [56]	[2], [4], [9], [13], [14], [16], [18], [28], [33], [34], [35], [44], [49], [51], [64]
DeFi Applications	[1], [7], [19], [20], [23], [24], [32], [36], [37], [46], [48], [50], [60]	[6], [8], [10], [11], [12], [14], [15],[17], [19], [20], [25], [27], [30], [37], [38], [41], [42], [43], [47], [48], [53], [55], [56], [57], [59], [62], [63], [69]	[34], [35], [38], [40], [42], [43], [53], [59], [62]
Blockchain Infrastructure	[3], [15], [19], [21], [22], [26], [31], [32], [39], [50], [51], [54], [56], [65]	[29], [31], [46], [50], [55], [66]	[22], [39], [49], [65]
Financial Industry	[5], [51], [52], [54], [58], [61]	[5], [7], [10], [51], [52], [58], [61], [68]	[58], [61], [68]

Table 2: DeFi research classification framework with IDs of literature items.
Source: Own illustration based on Risius and Spohrer (2017).

Table 3 depicts a heat map for our framework's relative number of classifications. Overall, there are 119 classifications (68 AL classifications and 51 GL classifications), while there are 69 identified literature items (45 AL and 24 GL) showing multiple classifications for one item.

Specifically, GL items have more multiple classifications (27) than AL items (12), suggesting that generally, a GL item covers more DeFi research topics than an AL item.

(a) Activities: It stands out that there is a concentration of literature in {Measurement & Value} (41%), closely followed by {Design & Features} (33%) and only 26% in {Management & Organization}.

(b) Level of analysis: It appears to be that there also exists a concentration of literature, this occasion in {DeFi Applications} (42%). The remaining groups are {Users & Society} (23%), {Blockchain Infrastructure} (20%), and {Financial Industry} (14%).[9]

Level of analysis \ Activities		Design & Features	Measurement & Value	Management & Organization
Users & Society	AL	4%	4%	18%
	GL	6%	8%	6%
	Total	5%	6%	13%
DeFi Applications	AL	13%	26%	9%
	GL	8%	20%	6%
	Total	11%	24%	8%
Blockchain Infrastructure	AL	13%	3%	3%
	GL	10%	8%	4%
	Total	12%	5%	3%
Financial Industry	AL	1%	4%	0%
	GL	10%	10%	6%
	Total	5%	7%	3%

Table 3: Classification heat map.
Source: Own illustration.

{Measurement & Value | DeFi Applications} is the category most popular among the entire set of literature. Furthermore {Management & Organization | Users & Society}, {Design & Features | Blockchain Infrastructure} and {Design & Features | DeFi Applications} is especially prominent in AL, while GL seems to be mostly balanced in distribution across the remaining categories. It is also noteworthy that AL seemingly is almost not represented in {Management & Organization | Financial Industry} and {Design & Features | Financial Industry}.

Further following the approach of Risius and Spohrer (2017), we will analyze the current state of knowledge and research trends by reviewing the identified literature and organizing them into our framework. ***Table 4*** depicts the major topics covered by the literature in each respective category.

9 There is a rounding error that leads to the sum of 99% instead of 100%.

	Design & Features	Measurement & Value	Management & Organization
Users & Society	User behavior in DeFi User groups DeFi features for users	Evaluation of risks Benefits / Disadvantages	Regulatory aspects in DeFi Illicit activities Analyses of proposed laws Regulatory outlook
DeFi Applications	AMMs Oracles On-chain derivatives Protocol DeFi features	Market efficiency Market manipulations Protocol security Crypto assets Token economics	Governance of protocols DAOs Governance tokens
Blockchain Infrastructure	Scalability Interoperability Consensus security Blockchain transparency Blockchain DeFi features	Comparison of platforms Transfer of value	Blockchain governance Miners
Financial Industry	DeFi services DeFi features for finance Value propositions	Evaluation of DeFi in finance Comparison of DeFi / CeFi Future for DeFi in finance	Convergence of DeFi and CeFi

Table 4: Major topics of the literature per category.
Source: Own illustration based on Risius and Spohrer (2017).

4.3.1 Design & Features

4.3.1.1 Users & Society

Work in this category focuses on how users perceive and interact with specific features of DeFi. User willingness to adopt is crucial for the advancement of concepts and technologies (Venkatesh et al. 2003). Hence, a key focus should lie in providing a better understanding of why users interact with a decentralized financial system and which features constrain or unchain usage. Our findings show that research in this field indeed tackles the key objective. Half of the work in this area covers this topic in a DeFi-overarching way, in which DeFi is viewed as an entity (Chanson et al. 2020; Chen and Bellavitis 2020; Lockl and Stoetzer 2021). The remainder of the works focuses on different DeFi platforms (Bashir et al. 2016; Irresberger et al. 2020) or specific protocols in DeFi (Aspris et al. 2021).

Chen and Bellavitis (2020) highlight the main features that may be generally trendsetting for user adoption, namely: decentralization, innovativeness, interoperability, borderlessness, and transparency. However, Lockl and Stoetzer (2021) find that users need to perceive a distinct added value when comparing DeFi to CeFi. Thus, it has to be evaluated if these features, in the way they currently exist, provide enough added value for user adoption. Remarkably, Lockl and Stoetzer (2021) do not find statistical evidence that distrust in banks fuels user adoption of

DeFi and conclude that users, although distrusting banks, seemingly do not care about resolving centralization trust issues if CeFi is more convenient. This is also because regulation safeguards CeFi and the DeFi protocol code may be unintelligible for the average user, thus reintroducing an element of trust (Lockl and Stoetzer 2021). Those results align with Bashir et al. (2016), finding that the lack of institutional embeddedness, which may counter this trust paradox, harms bitcoin adoption. While the aforementioned results may apply to all DeFi users, Aspris et al. (2021) and Irresberger et al. (2020) introduce the concept of group interests, indicating that there are different groups of participants in DeFi with different interests and needs. Irresberger et al. (2020) compare DeFi platforms in terms of adoption, scale, or security and conclude that only a few of them might be optimal for certain users because of their differentiating needs of those features. Aspris et al. (2021) investigate DeFi exchanges and find that their users face a choice between the anonymous, secure decentralized exchange (DEX) and the less secure, more liquid centralized exchange (CEX). Specifically, liquidity is of greater importance to traders with larger volumes. Until now, the literature has mostly considered the effects of design and features on user behavior; Chanson et al. (2020) are the first to address the effect of user interaction on user behavior. They find that discussion forums especially fill an essential role as signals to reduce information asymmetry and boost initial coin offering (ICO) participation.

4.3.1.2 DeFi Applications

The blockchain contains smart contracts and protocols that offer automated financial products and services on a P2P basis (See chapter 2.3). DeFi applications connect this blockchain back end with a user front-end. Therefore, work in this category targets the design, features, and implementations of those applications and their protocols. We find that the majority of literature in this category (1) deals with market makers to some degree (Angeris and Chitra 2020; Bartoletti et al. 2021b; Galal and Youssef 2021; Gawlikowicz et al. 2021; Lipton and Hardjono 2021; Pourpouneh et al. 2020; Zhou, Qin, Torres et al. 2021). The remainder of work in this category (2) focuses on various other protocols (Bahga and Madisetti 2020; Bartoletti et al. 2021a; Kroon et al. 2021; Kumar et al. 2020; Rius and Gashier 2020; Tien et al. 2020).

(1) Pourpouneh et al. (2020) investigate the efficiency of automated market makers (AMMs) and find that they rely existentially on arbitrageurs and the existence of efficient primary markets to balance the prices of AMMs with other markets, resulting in losses to suppliers of funds if there is a price gap that needs to be leveled. Hence AMMs need to be designed in a way that compensates liquidity providers by incentivizing mechanisms. These findings are in line with

the AMM literature (Angeris and Chitra 2020; Bartoletti et al. 2021b). Subsequently, Bartoletti et al. (2021b) and Gawlikowicz et al. (2021) provide formalizations, designs, and implementations of economic mechanisms for incentivizing liquidity and arbitrage. Zhou, Qin, Torres et al. (2021) research on market manipulation in AMM DEXs, finding that the feature of transparency in them opens up opportunities for market manipulation (especially for frontrunning and sandwich attacks). Preventing such manipulations proves difficult since increasing security (slippage protection) may hinder scalability (Zhou, Qin, Torres et al. 2021). Pourpouneh et al. (2020) are aware of this dilemma and mention a DEX with discrete clearing (batch auction) as a possible solution. Galal and Youssef (2021) tackle this dilemma and present a publicly verifiable and secrecy preserving periodic auction protocol that deploys zero-knowledge proofs and shows promising results in prototype testing concerning preventing the aforementioned manipulations.

The remaining AMM literature consists of two literature items that form a connection between AMM literature and the remaining heterogenous literature in this category. First, Kumar et al. (2020) introduce features for oracles necessary for trustworthy data on-chaining, namely: correctness of data, availability of data, and accountability of the data providers. Angeris and Chitra (2020) connect to that by introducing the concept of constant function market makers (CFMM) as oracles to overcome the oracle problem and synchronize on- and off-chain prices of assets. Second, Bahga and Madisetti (2020) introduce their implementation and design of a value token transfer protocol (VTTP) to facilitate intra- and inter-chain transfers of crypto assets. Lipton and Hardjono (2021) connect to that with their research on blockchain intra- and interoperability. They propose a concept that uses AMMs for intra-chain transfers and gateways / atomic swaps for inter-chain transfers of crypto assets. Necessary features of their protocol are the atomicity of transactions, consistency of ledgers, isolation of the asset, and durability of commitment (Lipton and Hardjono 2021). It is noteworthy that Lipton and Hardjono (2021) emphasize an increasing difficulty of protecting AMMs against threats inherited from the underlying smart contracts and tokens. We thus find that works with market makers as the main research objective are mainly concerned with attracting liquidity and ensuring the report of correct prices of crypto assets.

(2) Bartoletti et al. (2021a) introduce a concept of DeFi lending pools and their implementation details. Due to the absence of reputation and clear identification of participants in DeFi, it is not possible to give out loans on a trust basis; loans thus have to be overcollateralized (Bartoletti et al. 2021a; Kroon et al. 2021), which represents an issue of capital inefficiency (Tien et al. 2020).

To circumvent this Tien et al. (2020) propose that assets locked as collateral should be supplied to money markets to accrue interest and thus eliminate opportunity cost and capital inefficiency. Additionally, Tien et al. (2020) cover a mechanism in their concept that supplies locked collateral to money markets in case of an imminent liquidity crisis. Considering that collateralizing more than loaning out might defeat the raison d'être of a loan itself, Kroon et al. (2021) present their concept that aims to eliminate over-collateralization through the usage of self-sovereign identity (SSI) as collateral, meaning the possibility of using one's credit history for trust-based loans. Having now covered loans and exchanges, Rius and Gashier (2020) introduce a concept for "smart derivatives", specifically on-chain forwards. Their concept of a financial forward arises from an interplay of smart contracts and is fully collateralized. Additionally, it relies on a price oracle that feeds a contract the final price on expiry. An interesting feature of their approach is the inclusion of contracts in natural language that are then concatenated to the smart contracts by a hash (Rius and Gashier 2020). They conclude that their financial instrument may be exceptionally useful for hedging purposes despite their capital intensity.

4.3.1.3 Blockchain Infrastructure

This category is concerned with DeFi's underlying infrastructure, the blockchain. Respective questions and topics concern the design and features of the underlying platform relevant for DeFi. Work in this category can be broadly split into three classes. (1) Work that analyses and presents necessary blockchain features for DeFi (Amler et al. 2021; Brühl 2020; Chen and Bellavitis 2019; Qin, Zhou, Afonin et al. 2021), (2) work that discusses the consequences of these features (Aponte-Novoa et al. 2021; Galal and Youssef 2021; Li et al. 2021; Qin, Zhou and Gervais 2021; Zhou, Qin, Torres et al. 2021), and (3) work that introduces designs and concepts to improve these features (Han et al. 2019; Huili et al. 2021; Lipton and Hardjono 2021; Tefagh et al. 2020; Zhao et al. 2021).

(1) Qin, Zhou, Afonin et al. (2021) analyze the differences between CeFi and DeFi and outline DeFi properties. Features identified are public verifiability of code and events (transparency), asset custody, privacy (pseudonymity), atomicity of transactions, transaction order malleability, transaction fees, availability of service, and anonymous development. Chen and Bellavitis (2019) and Amler et al. (2021) concur with these features and add decentralization, interoperability, borderlessness, and trust-lessness (deterministic consensus to prevent double-spending). However, Qin, Zhou, Afonin et al. (2021) mention that it is possible for miners to (temporally) censor transactions and that migrating from CeFi to DeFi (on-ramping) or ramping-off typically

requires trusted centralized institutions (e.g: CEXs). The previous works are mainly concerned with public (permissionless) platforms. Brühl (2020) introduces libra (a DeFi system on a permissioned blockchain platform) and identifies scalability as a challenging factor that may hinder DeFi functionality. This finding also applies to public platforms (Amler et al. 2021). Now having covered the literature on features, we turn to the literature on consequences of these features.

(2) As already mentioned in {Design & Features | DeFi Applications} transparency enables attacks on transactions (Galal and Youssef 2021; Zhou, Qin, Torres et al. 2021). Attacks like frontrunning, back running, sandwich attacks, replay attacks, and clogging are reliant on specific transaction order and thus usually lead to a non-cooperative game of transaction fee bidding between adversaries, which makes them unattractive if a certain number of adversaries are existent (Qin, Zhou and Gervais 2021; Zhou, Qin, Torres et al. 2021). Miners, however, are a small subgroup of participants that hold the power to arbitrarily order transactions in a block or censor them in their block-building process; this enables them to circumvent the bidding game resulting in miner extractable value (MEV) and to shield themselves against aforementioned attacks by privately mining their transactions without ever publishing them in the P2P network. Qin, Zhou and Gervais (2021) find first evidence of miners exploiting MEV and private agreements between miners and other participants to mine transactions privately. They conclude by stating that these are worrying trends, considering that a competitive game of MEV between miners weakens blockchain consensus protocol security and that miners gain an unaccountable amount of influence through private agreement practices, possibly leading to centralization. This assumption is reinforced through Aponte-Novoa et al. (2021), which find an increasing concentration of hash-rate in the hands of a few miners and call for consideration of this finding in future designs of security protocols. Li et al. (2021) further state that detecting illicit behaviors in DeFi is particularly difficult since there is no guideline on what quantifies as illicit behavior but show that detecting it may be possible by making use of the blockchain transparency and proceeding to employ an algorithm on blockchain addresses that detects suspicious trades. While transparency and transaction order malleability thus seem to be problematic features, the literature on improvements does not target them.

(3) The literature on improvements of features is concerned with (i) interoperability and atomicity (Han et al. 2019; Lipton and Hardjono 2021; Tefagh et al. 2020), (ii) with scalability (Zhao et al. 2021), and (iii) with asset custody (Huili et al. 2021).

(i) Han et al. (2019) introduce the atomic swap, which is a sequence of conditional transactions that transfer assets from one platform to another (interoperability) and can only either fail or succeed (atomicity). The atomic swap requires the participating platforms to have hashlock and timelock functionalities for transactions to enable this atomicity. However, analyses in {Measurement & Value | Blockchain Infrastructure} show that the atomic swap in its original form is less of a swap and more of a financial option, being unfair to one participant without an associated premium. Han et al. (2019) thus design an improvement to make the atomic swap either a fair swap of assets or a fair option. They acknowledge that the time-lock suffers from unreliability since the timestamp accuracy in blockchains may differ. The atomic swap without optionality can also be used for a concept called “Atomic Bonded Cross-chain Debt” (ABCD), introduced by Tefagh et al. (2020), which is an uncollateralized cross-chain bond made possible by an atomic sequence of conditional transactions. They conclude by stating that their financial instrument is handy for arbitrage analogously to flash loans[10]. Lipton and Hardjono (2021) mention that atomic swaps rely on both participants to read the opposing ledgers and thus eliminate the usage with permissioned blockchains. They introduce the concept of gateway nodes for each blockchain and a gateway-to-gateway asset transfer protocol to circumvent this problem. The works on atomic swaps tend to agree on them being only as safe as the blockchains involved if they are facilitated by transactions; if they are facilitated by smart contracts, there is the additional risk of the contracts involved being flawed. Overall, it seems that atomicity enables interoperability.

(ii) Zhao et al. (2021) tackle the aforementioned blockchain scalability issue by proposing a block synchronization protocol that converts the raw transactions in a block to a single hash of them. This reduces the needed bandwidth, resulting in higher transaction throughput of the blockchain network. Specifically, the protocol can reduce the size of an Ethereum block by an average of 83.55% in performance analyses.

(iii) Huili et al. (2021) take on asset custody in blockchains. They design a dynamic threshold elliptic curve digital signature algorithm (ECDSA) that requires the agreement of multiple custodians before assets can be used. Furthermore, the proposed signature scheme supports adding and removing custodians from the custody procedure. An important application of this signature

[10] A flash loan is a conditional sequence of multiple transactions that is atomic by being grouped in a smart contract. The loan gets requested, used and payed back in one block, if not payed back the loan is not payed out.

may be in CEX since CEX hold the private keys of their users, thus making their assets susceptible to misappropriation (Huili et al. 2021).

4.3.1.4 Financial Industry

DeFi typically provides alternative financial services by usage of blockchains and DeFi applications. Having considered which features and designs potentially are relevant for users, we want to also consider the effects on the already existing financial industry in the following. Work in this category covers which concepts/designs and features make DeFi potentially disruptive for established financial firms and institutions. Literature in this category can be split into (1) Concepts of financial services in DeFi (Chen and Bellavitis 2019, 2020; Derviz and others 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021) and (2) Promising features of these services (Derviz and others 2021; Meegan and Koens 2021; Qin, Zhou, Afonin et al. 2021). As can be seen, there is an overlap in this division. Considering the topic of this category, we want to highlight that (Derviz and others 2021; Katona 2021; Meegan and Koens 2021) are works either written by employees of banks and/or in the name of banks.

(1) Concepts of financial services identified in DeFi are lending/borrowing, market-making, exchange of assets, payment services, contracting, portfolio management, insurance, and fundraising (Chen and Bellavitis 2019, 2020; Derviz and others 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021). However, Katona (2021) finds that DeFi currently does not offer the full range of CeFi services, while Qin, Zhou, Afonin et al. (2021) state that there also are services, like flash loans, that only exist in DeFi.

(2) Meegan and Koens (2021) research on potentially promising features of DeFi for financial services and find that composability, flexibility, decentralization, accessibility, innovativeness, interoperability, borderlessness, transparency, automation of business processes, and transaction finality are these aforementioned features. This finding is in line with Qin, Zhou, Afonin et al. (2021), which research several DeFi services and consider these features but find that the most differentiating features between both financial systems are transparency, control, and accessibility. Control means that users in DeFi are their asset custodians, and accessibility means that everyone can participate. Derviz and others (2021) raise that often-advertised features of DeFi are: banking underbanked regions, preventing risks of centralized financial systems, circumventing regulatory bans, financial innovation, and thus are in line with aforementioned features. We find that the entirety of literature in this category thus tends to agree on these properties. However, the names of them differ occasionally, or features are paraphrased. Furthermore,

there is an overlap of these financial features with the technical ones found in {Design & Features | Blockchain Infrastructure}. Uniformly the works mention that the aforementioned features also come with downsides. Most prominently, anonymity and decentralization may lead to asset custody and accessibility and thus facilitation of self-sovereignty, but create issues of enforcing regulatory measures (e.g.: know-your-customer (KYC) checks and anti-money-laundering (AML) laws) (Qin, Zhou, Afonin et al. 2021). Additionally, Meegan and Koens (2021) identify transparency as a feature in trade-off with privacy rights, and Qin, Zhou, Afonin et al. (2021) mention the negative impact of transparency on financial transactions, as already covered in {Design & Features | Blockchain Infrastructure}. Another interesting point is raised by Katona (2021), who mentions that the popularity of DeFi services drives gas fees up to and thus hinders accessibility to services and calls for solutions to the scalability issue. Meegan and Koens (2021) conclude that the aforementioned features may be beneficial theoretically; however, these benefits are not always realizable in practice. We conclude that, once again, transparency seems to be a problematic feature and that literature in this category mentions the regulatory uncertainty as prominent adoption hindering issue of DeFi in the financial service industry.

4.3.2 Measurement & Value

4.3.2.1 Users & Society

This category is concerned with evaluating DeFi’s value proposition for users. Work focuses on the question of what benefits/disadvantages are provided by using DeFi for single users as well as for society and the evaluation of these. We do not find a characteristic by which the literature can be meaningfully further subdivided in this category except that the majority mention both benefits and disadvantages (Amler et al. 2021; Bennett et al. 2020; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021), while one work focuses on risks only (Carter and Jeng 2021).

Chen and Bellavitis (2020) find that DeFi potentially can reduce transaction costs, facilitate financial inclusion and self-sovereignty of users. This is reinforced through consensus in the remaining literature that includes advantages of DeFi (Amler et al. 2021; Bennett et al. 2020; Chen and Bellavitis 2020; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021). Furthermore, they add increased efficiency and innovativeness to the advantages of DeFi. We find that the entirety of the literature agrees on these potential advantages, originating from designs and features (mentioned in 4.2.1) of decentralized finance (e.g.: financial inclusion through borderlessness and open-access). However, as already covered, these features come with downsides that turn into risks when using DeFi. We find that overall, the literature in this category concurs concerning the risks/disadvantages of DeFi. Identified risks can be classified into (1) Blockchain infrastructure risks, (2) Protocol risks, (3) Market risks, and (4) DeFi-overarching risks.

(1) Blockchain infrastructure risks originate from the blockchain itself; identified were limited scalability, MEV, transaction attacks, consensus failures, and privacy rights violations (Amler et al. 2021; Carter and Jeng 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021). Limited scalability refers to the limited throughput of a blockchain network, increasing gas fees for transactions and thus hindering accessibility. Transaction attacks (MEV being one of them) increase price slippage and extract value. Consensus failures refer to the security of the blockchain and its data consistency. Privacy rights valuations result from having to publish every transaction data.

(2) Risks identified regarding protocols are protocol dependencies, protocol vulnerabilities/manipulations, and re-centralization of protocols through admin keys or governance takeovers (Amler et al. 2021; Carter and Jeng 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021). Protocol dependencies result from composability and refer to the state of one protocol being influenced by another (e.g., oracles). Protocol vulnerabilities/manipulations include technical and economical design errors, making them unsafe to use or exploitable. Admin keys of protocols offer a backdoor for emergency takeovers but jeopardize decentralization and could also be used maliciously.

(3) On a market level, there are risks of market manipulations, illiquidity, volatility of assets, and re-centralization through central entities (Amler et al. 2021; Carter and Jeng 2021; Chen and Bellavitis 2020; Katona 2021; Qin, Zhou, Afonin et al. 2021). Market manipulations include price-oracle attacks, pump and dump arbitrage, and other frauds/scams. Illiquidity refers to markets draining out and hindering accessibility to financial markets and funds. The volatility of assets hinders financial transactions and deposits since they do not represent a store of value or stable means of exchange. Re-centralization on the market level refers to central entities in those markets (e.g.: DEX and stable coin reserves).

(4) DeFi-overarching issues are regulatory uncertainty, enablement of illicit activity, limited adoption/usability, and dependency on CeFi (Amler et al. 2021; Bennett et al. 2020; Carter and Jeng 2021; Chen and Bellavitis 2020; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021).

Regulatory uncertainty results from non-existent regulatory rules or guidelines on DeFi, presenting a risk that cannot be assessed. Through pseudonymity and decentralization in combination with financial markets, DeFi offers the potential to conduct illicit activities. Limited adoption/usability refers to yet still limited network effects and user-friendliness of DeFi. Dependency on CeFi refers to the circumstance that real-world business applications of DeFi often require centralized financial intermediaries (e.g.: silvergate bank, signature bank, fintech apps) that jeopardize decentralization and may represent single point of failures. These risks do not exist isolated from each other: like protocol's dependencies on each other (e.g.: as oracles) can lead to market manipulation by maliciously creating arbitrage opportunities (e.g.: bZx attack) (Amler et al. 2021; Carter and Jeng 2021), or MEV can lead to consensus failures as covered under {Design & Features | Blockchain Infrastructure}.

Having covered potential advantages and disadvantages, we want to analyze the literature in this category regarding an evaluation of these. Although agreeing on foundational benefits and disadvantages, the literature is split in their evaluation. Bennett et al. (2020), Chen and Bellavitis (2020), Katona (2021), Schär (2021) see DeFi potentially creating fundamental shifts in the economy and leading to a new financial paradigm. Specifically, the innovativeness and facilitation of self-sovereignty through decentralization and trustlessness are mentioned as the leading causes for the potential success of DeFi. Innovativeness means that DeFi provides room for experimentation, creation, and improvements of (new) financial services/instruments and facilitation of self-sovereignty, which refers to DeFi putting the power into the hands of the respective users. Amler et al. (2021), Carter and Jeng (2021), Qin, Zhou, Afonin et al. (2021) see the added value of DeFi as more conservative. Carter and Jeng (2021) find that DeFi inheres traditional financial risks plus DeFi-specific risks and conclude that DeFi struggles to attain perceivable real-world usefulness, which is in line with Amler et al. (2021). Qin, Zhou, Afonin et al. (2021) conclude after analyzing differences between CeFi and DeFi that the value proposition of both systems may be close to each other. Although their differences in evaluation of benefits and risks, the entirety of work concurs that for DeFi to work at a baseline, mainly regulatory uncertainty, scalability, and security overall must be addressed (Amler et al. 2021; Bennett et al. 2020; Carter and Jeng 2021; Katona 2021; Qin, Zhou, Afonin et al. 2021; Schär 2021).

We acknowledge that some of these risks can be elements of others, like market manipulation being a part of illicit behavior. However, illicit behavior includes various other elements (e.g.:

scams), and we aim to give an overview of risks identified in the analyzed literature, leaving a comprehensive taxonomy for future works.

4.3.2.2 DeFi Applications

Work in this category conducts evaluations on a DeFi application level. Considering the aforementioned requirements for DeFi to work at a baseline, an important question is if protocols and services and their respective markets are secure and effective/efficient. Furthermore, the work in this category sheds light on values (tokens/assets) that originate from these protocols. This is the category mostly targeted by literature on DeFi, as the preliminary analysis in the descriptive overview showed (see **Table 2**). We find that it is possible to split works in this category based on their primary research object: (1) targets specifically DeFi protocols (Angeris and Chitra 2020; Aspris et al. 2021; Caldarelli and Ellul 2021; Cao et al. 2021; Gudgeon, Perez et al. 2020; Gudgeon, Werner et al. 2020; Huili et al. 2021; Li 2021; Pourpouneh et al. 2020; Wang, B. et al. 2021; Zhou, Qin, Cully et al. 2021; Zhou, Qin, Torres et al. 2021), (2) is concerned with DeFi protocols and tokens (Amler et al. 2021; Bartoletti et al. 2021a; Brennecke et al. 2022; Jensen et al. 2021; Klages-Mundt et al. 2020; Nadler and Schär 2020; Perez et al. 2021; Schär 2021; Tolmach et al. 2021; Victor and Weintraud 2021; Wachter et al. 2021) and (3) is concerned explicitly with tokens (Corbet et al. 2021; Liu et al. 2020; Saengchote 2021; Silberholz and Di Wu 2021).

(1) Angeris and Chitra (2020) and Pourpouneh et al. (2020) research on AMMs and evaluate them generally as inefficient because they rely on external arbitrageurs to synchronize asset prices with primary financial markets, which result in losses for liquidity providers that need to be compensated by interest rates/collected service fees. However, Angeris and Chitra (2020) find that arbitrageurs are sufficiently incentivized to synchronize prices and Pourpouneh et al. (2020) find that AMMs work exceptionally well for assets with high liquidity and low volatility and that AMMs nevertheless fulfill an essential role in facilitating automatically market-making, fast trades and being composable building blocks for DeFi. AMMs can be used in lending protocols, which are researched by Gudgeon, Perez et al. (2020) and Gudgeon, Werner et al. (2020). Gudgeon, Werner et al. (2020) research on the employed interest models and resulting liquidities in those protocols. They find that these interest models are the main mechanism to incentivize liquidity in times of high utilization (low liquidity) and borrowing in times of low utilization. They proceed by analyzing different lending protocols (dYdX, Compound, Aave) and find that there are times where those are near-illiquid, making suppliers unable to withdraw

their funds. Overall, it seems that those times of illiquidity are shared across protocols although differing interest rate curves and that only a small number of addresses own a significant majority of locked funds, making them able to control liquidity in those protocols (Gudgeon, Werner et al. 2020). They also find that borrowing rates of different lending protocols influence each other (with Compound having market power and dictating these changes), indicating that participants are incentivized to switch between them. They conclude by stating that those protocols may not be fully capital-efficient but highlight that this may also be the case in traditional foreign exchange markets. This makes borrowing a low-yield asset to obtain high-yield assets a potentially profitable strategy, and that since markets in those protocols are inefficient, participants may not fully respond to incentive mechanisms. Gudgeon, Perez et al. (2020) find that such protocols can become uncollateralized with sufficient illiquidity, and insolvency can occur quickly. Further, they show that if such protocols are decentrally governed by decentralized autonomous organizations (DAOs), it is possible to attack the governance mechanism by obtaining/holding a significant amount of governance tokens, which may be made be possible through flash loans (and if they are not governed decentrally an element of trust is re-introduced). Their work is concluded by stating that those aforementioned economic problems and the attacks are most likely to be mutually enforced, meaning one can lead to the other and vice versa.

Aspris et al. (2021), Huili et al. (2021), Zhou, Qin, Torres et al. (2021) cover DeFi exchanges. Specifically, Zhou, Qin, Torres et al. (2021) deal with AMM DEXs, finding that they currently have a security/scalability trade-off to solve, as explained in {Design & Features | DeFi Applications}. Aspris et al. (2021) and Huili et al. (2021) connect to that by covering differences between DEXs and CEXs. Aspris et al. (2021) find that DEXs are especially useful for obtaining capital in smaller/younger projects, while CEXs fulfill a gatekeeper role, certifying the quality and credibility of different projects and that there might be a user segmentation between both exchanges. They conclude by stating that a DEX may fulfill a price-discovery function and are mainly on-ramps for projects to regulated CEXs with higher trade volumes. However, transferring assets to a CEX implies giving away custody of them and impairs security (Aspris et al. 2021; Huili et al. 2021). In a way, there is thus a trade-off between security and scalability once again (this time not on a transaction level, but an asset level).

Having now considered the single protocol literature, we analyze the protocol-overarching literature. Zhou, Qin, Cully et al. (2021) research on profit-generating transactions across the intertwined protocols in DeFi. They employ two tools to detect those transactions, one for arbitrage purposes (cyclic transactions) and one for various other transaction pathways (non-cyclic). They find that all identified transactions are profitable, considering that the only cost are transaction fees and that the requirement to hold initial base assets can be reduced to < 1 ETH when using flash loans. Most notably, their tool for non-cyclic profit-generating transactions can identify a pump and arbitrage attack (specifically the bZx attack). Zhou, Qin, Cully et al. (2021) state that the bZx attack was found to exceed the average block reward for miners by 874 times (1,735,048 USD extracted); the next highest profitable transactions only yielded 31 and 8.5 times the average block reward. However, they research when a single miner would try to extract this value by forking the chain and find that this is already the case when an opportunity exceeds the block reward by 4 times. They conclude that most profitable transactions thus have worrying implications concerning consensus security.

Cao et al. (2021) are also aware of the role that flash loans play in enabling attacks by reducing the costs of conducting them. They thus research flash loan attacks (mainly bZx) and how flash loans interact with the mesh of protocols in DeFi. The attacks are classified mainly “Pump and Arbitrage” or “Oracle Manipulation”. The main contribution of Cao et al. (2021) hereby consists in clearly showing the connection between protocols in such attacks and the proposal of a standardized “asset flow diagram”. They find that the success of flash loan attacks is owed to the high degree of automation and transparency/predictability of code (Cao et al. 2021). Additionally, they highlight that although the main target of such attacks are AMMs, they do not play the leading role in the attack and get targeted because often AMMs act as decentralized price-oracle for other protocols, making it possible to manipulate asset exchange rates. They see a trend of pump attacks focusing on low liquidity asset pairs and thus reason that the size of the liquidity pool of AMMs will determine the level of market security against such attacks.

Wang, B. et al. (2021) present their work on DeFi attacks and their proposed tool to detect such. It considers oracle dependencies of the protocol as potential vulnerability and analyzes transactions conducted with the protocol to detect attempts for attacks. The tool found 37 to 124 (depending on slippage threshold) suspicious transactions in 150.871 Ethereum blocks. They also consider the bZx attack as an example and highlight that the main steps of the attack were exploiting the oracle dependency to control exchange rates and then exploiting them by pump and arbitrage, thus being in line with the previous works (Cao et al. 2021; Zhou, Qin, Cully et al. 2021). Furthermore, Cao et al. (2021), Wang, B. et al. (2021), Zhou, Qin, Cully et al. (2021)

agree on composability and transparency being the main contributors for those attack vulnerabilities, while flash loans mainly provide a means of obtaining enough funds at a negligible cost to leverage on them. Cao et al. (2021) conclude by stating that such attacks may be prevented if flash loans are constructed to facilitate buying and selling operations in different blocks (while acknowledging that increasing slippage protection in protocols may be fruitless). They state that those attacks have shown several weaknesses in DeFi and thus provide a tool to speed up improvements. Li (2021) covers smart contracts in general concerning market efficiency. They find that theoretically, smart contracts can facilitate market efficiency better than traditional markets, however for them to do so, the oracle and scalability problems need to be solved, and smart contract vulnerabilities need to be addressed. This finding aligns with the issues mentioned in the previous works in (1).

Having covered works on protocols, we analyze literature that connects protocols with crypto assets/tokens (2). Carter and Jeng (2021) are also in line with the smart contract vulnerabilities identified by Li (2021). However, they research various protocol risks and further identify interconnections with traditional financial systems as a risk category. Most notably, they identify stablecoins as a potential point of failure, resulting from institutions holding reserves that back the value of the stablecoin and enable it to maintain its peg but re-introduce a trust element because the institution controls the currency (Carter and Jeng 2021). They are also aware of stablecoins not backed by reserves (non-custodial), which maintain their peg by on-chain collateralizing (Carter and Jeng 2021; Klages-Mundt et al. 2020; Schär 2021) and find that they are more resilient and secure when using a native asset (e.g.: Ether) as long as its volatility is managed but become rather insecure again when using other assets as collateral. This finding is in line with previous literature on stablecoins (Klages-Mundt et al. 2020; Schär 2021). Klages-Mundt et al. (2020) add that especially non-custodial stablecoins are generally vulnerable to governance, price-oracle, and MEV attacks, and stablecoins in general for smart contract vulnerabilities and protocol dependencies. MEV hereby could have a twofold impact on stablecoins: first, it destabilizes the stablecoin by exploiting liquidation opportunities, and second, it impacts the blockchain native asset (which is often used for stablecoin collateral), destabilizing the stablecoin.

While these issues have been discussed before, we want to highlight governance issues in stablecoin systems. Governance in those protocols is tasked with adjusting the system parameters. This can be done either by agents, decentralized voting, or algorithms (Klages-Mundt et al.

2020). They find that every mode of governance has its fair share of disadvantages. While algorithmic governance is found to be exceptionally susceptible to oracle attacks, governance by agents re-introduces counterparty risk (trust), and governance by decentralized voting focuses less on the system's stability but more on maximizing profits. This finding is in line with Brennecke et al. (2022), which analyze the MakerDAO stablecoin system and conclude that "MakerDAO does not appear to replicate the primary goals of a central bank, namely price stability, support of economic activity, and a reduction in unemployment, but provides a valuable step towards a more stable DeFi ecosystem" (Brennecke et al. 2022). That stablecoins are indeed needed and valuable for the DeFi ecosystem is reinforced by Schär (2021), who identifies native assets as too volatile to function as a store of value and means of value exchange, being the reason for the creation of the first stablecoins.

Caldarelli and Ellul (2021) research on the oracle problem in DeFi and identify two types of oracles: centralized oracles are protocols for on-chaining information controlled by a single agent, and consensus oracles are decentralized voting protocols in which a group of agents has to come to a consensus on information that is going to be on-chained. Caldarelli and Ellul (2021) divide the oracle problem in a technical dimension (e.g.: oracle having design flaws) and in a social dimension (e.g.: oracle being manipulated by agents). They argue that the oracle problem in DeFi refers explicitly to data of assets and them being altered either by disfunction or manipulation. Through the approach of an MLR, they identify applications that need oracles: lending pools, AMMs, stablecoins, and derivatives. This insight is in line with our previously analyzed literature of those applications in this category as well as in {Design & Features | DeFi Applications}. Oracles in lending pools are crucial to feeding prices of assets (e.g.: collateral) into the protocols. AMMs can act as decentralized oracles, but as already mentioned, they are vulnerable to flash loan/pump and arbitrage attacks. Caldarelli and Ellul (2021) mention that the Uniswap AMM has already implemented a time-weighted price feed, making them more resilient against the aforementioned attacks and more reliable as price-oracles for other protocols. Furthermore, those decentral, improved price-oracles can help ease the losses of suppliers in AMMs caused by arbitrageurs by limiting arbitrage actions. In line with the literature on stablecoins Caldarelli and Ellul (2021) find that custodial stablecoins do not require oracles. However, non-custodial stablecoins need them for feeding the price of collaterals and the discovery of the stablecoin/collateral ratio. In derivatives, oracles are used for feeding data between different DeFi platforms. It is found that oracles are susceptible to a variety of societal manipulations by the agents that are selected to participate in those oracles; the only technical vulnerability is malfunctions caused by the flawed design of protocols (Caldarelli and Ellul 2021). They conclude that oracles are vital as intermediaries between the deterministic "blockchain world" and the real world; however, they re-introduce trust and are not secure as a single point of failure.

These connections between AMMs as oracles, lending pools, and stablecoins are further confirmed by Bartoletti et al. (2021a). Perez et al. (2021) research on lending pools (specifically Compound) with a focus on governance tokens, which are supplied to users for participating. They find that risk-seeking behavior has spiked with the introduction of the governance tokens, as amounts borrowed are now significantly higher than before while maintaining a low collateral ratio leading to increased liquidation risk of those collateralized debt positions. Besides, they conclude that lending protocols have become increasingly efficient, although few control the amounts borrowed/supplied. We find that those results are thus in line with, and reinforced by, the previous literature (Gudgeon, Perez et al. 2020; Gudgeon, Werner et al. 2020).

On a more general level, Victor and Weintraud (2021) are the first to inspect DEX and their tokens regarding wash trading and find that this is quite typical behavior with a manipulated trading volume of 159 million dollars. Most notably is the insight that tokens tend to be wash traded the most at the beginning and end of their life cycle. However, they mention that wash trading saw a decline with the introduction of AMM DEXs but conclude that there is a strong incentive for wash trading, possibly finding a new way to conduct such on AMMs. For DEXs that are not AMMs, they propose a self-trade prevention functionality to lower those wash trades.

Amler et al. (2021), Jensen et al. (2021), Wachter et al. (2021) cover token distribution over various protocols. Wachter et al. (2021) find a trend towards complex wrapping operations across different protocols, meaning that assets of one protocol are supplied to another, obtaining a new derivative token that is then again supplied to a protocol, and so on. They suggest that this could be an indicator for deep DeFi integration of an asset and/or potential unnecessary additional risk. Further, they find that ownership of governance tokens is concentrated in the hands of few, potentially endangering the benefits of DeFi, and argue that yield farming is the leading cause for the growth of DeFi. They conclude that the complexity of DeFi has significantly increased, and main drivers for this vary significantly depending on the tokens. That governance tokens seem unbalanced in distribution and their distribution being somewhat centralized is in line with previous works (Amler et al. 2021; Jensen et al. 2021). Tolmach et al.

(2021) consider the composability of DeFi protocols and reinforce the finding that composability and the wrapping process enable additional attack vectors on DeFi protocols. They propose their formal analysis tool for composable DeFi protocols, which evaluates these with regards to undesirable interdependency conditions.

(3) Having covered literature that connects tokens to DeFi protocols, we turn to the literature that specifically covers tokens. Liu et al. (2020) and Saengchote (2021) hereby target specifically stablecoins. They try to document flows of the DAI stablecoin and find that this is a very intricate task due to the complex and intertwined DeFi system, possibly creating enormous challenges for accountants and legal requirements. Additionally, they are in line with the aforementioned findings that DeFi growth may be mainly facilitated by yield chasing opportunities that result from high composability and wrapping of assets. Liu et al. (2020) take on operational and market risks of stablecoins and find that the risk management of those systems (mainly conducted by decentralized voting) lacks scientific guidance and propose that traditional finance risk assessment practices should be adopted to increase security and stability. We find it worthy to mention that Brennecke et al. (2022) propose widening the scope of research to "real-world" collaterals in the form of tokens (e.g.: non-nonfungible tokes (NFTs)), and we argue that this is in line with the aforementioned inclusion of traditional financial tools to improve stable coins.

In line with identified challenges to accounting Corbet et al. (2021) ask if DeFi tokens are a separate asset class from native assets. To find out, they conduct evaluations on those assets' financial properties, finding that DeFi bubbles originate mainly from DeFi protocol tokens but also partly by the underlying blockchain's native asset, indicating that DeFi is mainly a separate asset with linkages to the native assets. They find that Bitcoin has a relatively limited causal relationship to DeFi tokens (while Ethereum has a significant causal relationship) and that MKR (stablecoin) and LINK (oracle) tokens have fundamental influence in the DeFi token space. They conclude that to diversify the risk of a crypto portfolio, one needs to consider both native assets and DeFi assets. We find that these findings once again reinforce the critical position of stablecoins and oracles, this time on an asset level, while previously analyzed literature mentioned their significant importance on an applicational level.

Silberholz and Di Wu (2021) take on the potential growth factors of DeFi and ask, "How much of the current boom is about real adoption and utilization of the technology, as opposed to pure speculation?" (Silberholz and Di Wu 2021). The answer to this question will most likely also determine whether DeFi growth is sustainable in the long run (Nadler and Schär 2020; Silberholz and Di Wu 2021). We find it helpful to elaborate roughly on what is meant by utility and speculation usage before proceeding to findings: speculation usage refers to moving assets to obtain potential profits, and utility usage refers to the moving of assets that is caused by simply using protocols (for a more detailed explanation, see Silberholz and Di Wu 2021, chapter 3.1.). They find that the utility usage sharply declined over time to about 5% of the weekly circulating tokens but has started to recover slightly after the DeFi boom in 2020. With the decline in utility, usage came a correspondingly sharp increase in speculative turnover. They highlight that speculation on CEXs has declined and transmitted to DeFi protocols (e.g.: on-chain derivatives, lending pools) after the DeFi boom, indicating that DeFi has a "crowding-out effect on both token utility and exchange-based speculation" (Silberholz and Di Wu 2021) facilitated by taking up the limited block space of the infrastructure. They are in line with the aforementioned literature finding that investors become increasingly risk-seeking, and the primary use of DeFi protocols currently is the speculation with tokens and its "yield farming" functionality. This is particularly worrying as higher utility usage is found to enable improved price discovery and lower future volatility of token prices (Silberholz and Di Wu 2021). The works, however, do not answer the question of whether DeFi growth is sustainable.

We acknowledge that there may be an intuitive and alternative way to structure this category into (1) stablecoins, (2) governance tokens, (3) various other protocols and tokens. The advantage of this structure mainly lies in agglomerating the findings on each topic. However, it fails to account for the connection between protocols and assets in a way in which it is represented in the chosen structurization. We find the chosen structure more suitable since the findings are still available (just more dispersed), and these connections are accounted for.

4.3.2.3 Blockchain Infrastructure

Measurement and value on a blockchain level is concerned with (1) evaluating benefits/disadvantages of platforms, and what surplus different DeFi platforms provide (Carter and Jeng 2021; Irresberger et al. 2020) and (2) how transferring value between them can be managed (Bahga and Madisetti 2020; Han et al. 2019; Lipton and Hardjono 2021; Wang, Z. et al. 2021).

(1) Irresberger et al. (2020) analyze different blockchains and find that only a few dominate specific applications. This is due to the respective platforms being leaders either in terms of adoption, scale, or security (or a double combination of them). They do not find evidence for a platform that can claim a monopoly in all three categories, so no single platform dominates all

blockchain applications. However, Ethereum is found to be the dominant platform for DeFi applications since it provides customers with complex financial instruments, and that Bitcoin has no value for most DeFi clienteles because of its limited functionalities. In terms of transaction throughput (scalability), it is found that all platforms (no matter the consensus mechanism) are inferior to traditional finance settlement methods (e.g.: VISA). Furthermore, those DeFi systems may have a systematic risk vulnerability stemming from the underlying blockchain by MEV, consensus failures, and miner centralization as well as flawed blockchain code, as often mentioned before in {Design & Features | Blockchain Infrastructure} and by (Carter and Jeng 2021).

(2) Bahga and Madisetti (2020) find that existing blockchain platforms lack interoperability and lack ways of transferring value between those. An essential tool to enable this interoperability is the atomic swap, as mentioned in {Design & Features | Blockchain Infrastructure}. However, they are evaluated as financially unfair (Han et al. 2019; Wang, Z. et al. 2021) because of their optionality (see {Design & Features | Blockchain Infrastructure}). Lipton and Hardjono (2021) add that further technical problems make atomic swaps only feasible between public blockchains and conclude that there are still hurdles to overcome for blockchain interoperability.

4.3.2.4 Financial Industry

Work that covers the evaluation of DeFi in comparison to the traditional financial ecosystem can be found in this category. Considering the ambitions of DeFi and its background, an important question that works in this category should answer is if DeFi will replace the traditional system or how these two systems will affect each other. We find no meaningful division criteria between works of this category.

Every literature item in this category highlights the origin of DeFi in some form or another with the emergence of Bitcoin from the world financial crisis of 2007, the fading trust in banks, and its corresponding aim to decentralize financial services and intermediation (Chen and Bellavitis 2020; Derviz and others 2021; Katona 2021; Kumar et al. 2020; Lockl and Stoetzer 2021; Meegan and Koens 2021; Qin, Zhou, Afonin et al. 2021). Kumar et al. (2020) further add that DeFi aims to replicate all the traditional financial instruments and services. Lockl and Stoetzer (2021) research on this distrust in banks and the connection to DeFi, further elaborating that distrust refers to the suspicion that intermediaries do not act in one's best interest (a typical principal-agent problem). As mentioned under {Design & Features | Users & Society}, they find that paradoxically users might not trust in DeFi, potentially hindering its adoption and that if it is more convenient and state of art to use CeFi, they will not consider the switch. This leads them to the conclusion that integration of DeFi into an institutionalized setting might ease the trust issue and that DeFi applications should focus more on interoperability and high convenience for customers than repeating decentralizing intermediation as a value proposition.

Chen and Bellavitis (2020) concur with that finding and introduce four major business models of DeFi, namely: decentralized currencies, decentralized payment services, decentralized fund-raising, and decentralized contracting. All of them are constructed with the intention to fix issues of CeFi in those areas. Especially the aspect of decentralized currencies with regard to fixing control and devaluation (inflation) issues of fiat currencies are often mentioned across the literature items (Chen and Bellavitis 2020; Derviz and others 2021; Kumar et al. 2020; Qin, Zhou, Afonin et al. 2021). Kumar et al. (2020) state that “Banks are getting more and more expensive for retail users charging various kinds of fees, reducing the number of free interactions, lowering the rate of interest on the savings account. To top it all fiat currencies, have no fixed supply, the government can any day start printing more money […] risking high rates of inflation [and] reducing the worth of money deposited in bank accounts” (Kumar et al. 2020). Qin, Zhou, Afonin et al. (2021) argue that on the flipside (well-managed) inflation is needed to keep a financial system scalable to growing demands and future economic activities. They argue that Bitcoin will thus potentially hinder economic activities in its future with its fixed supply schedule (21 million Bitcoin limit, while Ether has an inflation rate of approx. 4%). Native cryptocurrencies (BTC, ETH, etc.) have proven to be very volatile in value, restricting their function as means of exchange and store of value (Chen and Bellavitis 2020; Qin, Zhou, Afonin et al. 2021). The theoretical solution to that issue are stablecoins, which are pegged to fiat currencies and can be either centralized (through a reserve) or decentralized (by collateralizing or algorithms). However, Qin, Zhou, Afonin et al. (2021) find that the reserve mechanism is the most stable and the algorithm the least stable. As shown in {Measurement & Value | DeFi Applications}, decentralized stablecoins have additional issues like governance, oracles, and various other attack vectors, while centralized stablecoins re-introduce trust in a central party.

Decentralized payment service refers to theoretical, cost-reducing, and border-less P2P payments between parties (Chen and Bellavitis 2019). Chen and Bellavitis (2019) argue that new business models based on micro payment may become possible with enough transaction cost reduction. However, if DeFi can reduce transaction costs remains an open question which outcome is based on blockchain scalability (Katona 2021; Meegan and Koens 2021).

Decentralized fundraising refers to the possibility of raising funds for a project via DeFi. Chen and Bellavitis (2019) identify initial coin offerings (ICOs) and initial exchange offerings (IEOs). The main difference between them is that IEOs are ICOs that an exchange vouched for (in terms of trustworthiness). Fundraising is especially valuable when a token has inherent utility in a DeFi project (Chen and Bellavitis 2019).

The last business model raised was decentralized contracting, which refers to decentralized autonomous financial "intermediation" (e.g.: lending/borrowing), which may reduce costs and enable innovations. These business models are furthermore in line with those identified by Derviz and others (2021). Derviz and others (2021), Meegan and Koens (2021), Qin, Zhou, Afonin et al. (2021) also cover decentralized lending more specifically. Meegan and Koens (2021), Qin, Zhou, Afonin et al. (2021) mention that in a pseudonymous environment, over-collateralization is the only feasible tool against counter-party default and that deposited assets are not protected by traditional finance safeguards (e.g.: laws like the deposit guarantee act). Meegan and Koens (2021) add that it is unclear if DeFi protocols fulfill the role of banks at all. Those findings are also in line with Derviz and others (2021) that compare DeFi to CeFi lending and further conclude that DeFi remains mainly "a playground for professional crypto speculators [which] business model has become known as yield farming" (Derviz and others 2021).

We find it necessary to point to the research on DeFi growth in {Measurement & Value | DeFi Applications}, which concluded that the main incentive for using DeFi currently are high return rates and the resulting "yield farming". Derviz and others (2021) state that these lucrative opportunities are expected to become scarcer as DeFi matures, which is in line with the literature on DeFi growth. Further, Katona (2021), Qin, Zhou, Afonin et al. (2021) agree that there are DeFi specific risks that mainly are facilitated by its technology and are not represented in traditional finance to such extents, namely: transaction attacks, protocol vulnerabilities, dependencies, enablement of illicit activities and regulatory uncertainty. Zetzsche et al. (2020) take on the regulatory aspect of DeFi. They argue that DeFi will come with centralized points in its system and that rather than eliminating the need for regulations, DeFi requires it to achieve a secure degree of decentralization. We find that the entirety of works comes to the same conclusion: DeFi will most likely not replace traditional finance. However, it theoretically provides enough promising features for the financial industry that both systems will most likely co-exist and learn from each other (Chen and Bellavitis 2020; Derviz and others 2021; Katona 2021; Kumar et al. 2020; Lockl and Stoetzer 2021; Meegan and Koens 2021; Qin, Zhou, Afonin et al.

2021). Before becoming a viable financial system, however, the issues of DeFi have to be addressed, which are mainly: facilitating adoption, tying real-world assets to DeFi, preventing illicit activity, enhancing DeFi security, and reducing regulatory uncertainty (Chen and Bellavitis 2020; Derviz and others 2021; Katona 2021; Kumar et al. 2020; Lockl and Stoetzer 2021; Meegan and Koens 2021; Qin, Zhou, Afonin et al. 2021).

Derviz and others (2021) raise the interesting possibility of using central bank digital currencies (CBDCs) as reserve-backed stablecoins to bridge traditional finance with its fiat currencies and DeFi with its crypto currencies. Such a proposal to bridge DeFi and CeFi on re-centralized points in DeFi to tackle its issues by trusted traditional financial institutions is also suggested by previous literature (Meegan and Koens 2021; Qin, Zhou, Afonin et al. 2021; Zetzsche et al. 2020) and might address a fundamental question that cannot be answered in a fully decentralized system: Who is responsible? (Qin, Zhou, Afonin et al. 2021). Furthermore, Meegan and Koens (2021) argue that a fully decentralized system may be suboptimal because of detrimental distribution of assets, poor efficiency, and poor stability, as well as a fully centralized one that suffers from inherent weaknesses of every trust-based model. Thus, they also conclude that combining both systems potentially serves the common good for financial users.

4.3.3 Management & Organization

4.3.3.1 Users & Society

Work categorized into this category deals with the management and organization of DeFi regarding its users and society. Under this category, mainly works of regulators and lawmakers can be found, as well as analyses of proposals for regulations. Considering previous findings and those in {Measurement & Value | Financial Industry}, we argue that important questions to be answered should be how regulators address issues of DeFi, why regulatory uncertainty exists and how it can be resolved. We find that literature can be further split into (1) works that analyze DeFi concerning regulatory aspects (Bennett et al. 2020; Doan et al. 2021; Guseva 2021; Qin, Zhou, Afonin et al. 2021; Suga et al. 2020; Ushida and Angel 2021; Zetzsche et al. 2020), (2) works that cover already proposed regulations (Maia and Vieira dos Santos 2021; Taylor 2021; Wright and Meier 2021) and (3) works that propose further directions for lawmakers and regulators (Hughes 2021; Matsuo 2020; Schrepel and Buterin 2020; Takanashi 2020; Victor and Weintraud 2021).

(1) Qin, Zhou, Afonin et al. (2021) cover the DeFi on-boarding and its compliance process and find that on-boarding to DeFi typically requires a CeFi intermediary (e.g.: CEXs). KYC is required for CeFi institutions and firms by regulators so that the identity of their customers can be verified and their intents for using financial services clarified. KYC is found to be very helpful for combating illicit activities, but on the other hand, increases costs of service provision (Qin, Zhou, Afonin et al. 2021). They additionally identify AML verifications as continuous compliance efforts in CeFi to prevent money laundering by verifying the source, destination, and purpose of asset transactions. Qin, Zhou, Afonin et al. (2021) argue that the on-boarding process over a central point links the pseudonymous address to the "real world" identity, and because of the transparency property, it is then possible to trace every transaction much easier. However, they acknowledge that it is also possible to bypass all of this by solely operating in DeFi or using Mixers but moving non-checked assets back into CeFi is still very difficult. Zetzsche et al. (2020) also find that centralization is often at the heart of decentralization and that regulation will mainly focus on these points to apply its pressure to enforce laws. Furthermore, they mention that emergency support (like a lender of last resort, deposit guarantee schemes) may not be feasible in a decentralized system. They conclude that since DeFi is inherently border-less and decentralized, it may not be easy to apply an integrating DeFi regulation since it exists in multiple jurisdictions and call for a multilateral approach, proposing that DeFi regulation may be embedded in its protocol code to facilitate regulated decentralization. Another interesting point raised by Qin, Zhou, Afonin et al. (2021), and Zetzsche et al. (2020) is that data privacy laws (e.g.: GDPR's "Right to be forgotten") may be violated by the blockchain technology that underlies DeFi and stores ever transaction publicly.

That there exist accountability and enforcement issues concerning regulations and laws in DeFi is a common finding between the works in this category (Bennett et al. 2020; Doan et al. 2021; Guseva 2021; Qin, Zhou, Afonin et al. 2021; Ushida and Angel 2021; Zetzsche et al. 2020). Guseva (2021) analyzes the role of the Securities and Exchange Commission (SEC) in DeFi and finds that depending on how assets are classified, the SEC might not have jurisdiction. The SEC started its enforcement of regulations with the "DAO Report" of 2017 and uses court cases and administrative proceedings to pursue charges. Interestingly, they not only charge entities (e.g.: a DAO/service) but also its natural persons (e.g.: founders, insiders, etc.), which are mainly charged with violation of registrations (e.g.: offering governance tokens without registration for a securities offering) (Guseva 2021). It is found that the SEC requires the cooperation of the agents in DeFi to not lag behind on DeFi innovations and that if regulatory actions remain unpredictable, it will be hard to attain such cooperation between regulatory bodies and the DeFi realm. Ushida and Angel (2021) raise that there are additional aspects of DAOs that need to be considered by regulators. They argue that currently, it seems that a value proposition of DeFi is its non-compliance with laws and that considering the growing regulatory scrutiny, some of the DeFi projects might choose cooperation while others might pursue further decentralization, eluding regulatory addressability. Ushida and Angel (2021) mention cases of DAOs that are also represented off-chain as legal entities (e.g.: limited liability companies) and aim to reduce regulatory uncertainties in the course of this. However, they are aware that this indicates a tradeoff between regulatory compliance and decentralization. Further mentioned issues of DAOs are admin keys, governance tokens, and various other re-centralized points, and Ushida and Angel (2021) propose regulatory actions to ease these issues. We want to highlight that those issues are common issues of DeFi protocols as shown in {Measurement & Value | DeFi Applications} and the proposal to fix those with trusted entities (here: regulatory bodies) is in line with works in {Measurement & Value | Financial Industry}.

It is possible to incorporate regulatory entities in DeFi by demanding an admin key, obtaining governance tokens, and applying pressure to centralized points (e.g.: CEXs, oracles) (Ushida and Angel 2021). However, they mention that one should be exceptionally careful with admin keys since they require careful security measures regarding their storage and accessibility. Regarding governance tokens, it is found that a major problem currently is that they can be classified as securities that might not account for their unique functions in a protocol. Ushida and Angel (2021) conclude that there is a real need for assessing the nature, function, and risk of DeFi assets and associated motivations to obtain them, which is in line with Guseva (2021). This finding is reinforced by Doan et al. (2021), which research on NFTs, and by Bennett et al. (2020), which survey accountants, regulators, auditors, and other practitioners. Both works mention that it is a non-trivial task to classify crypto assets into existing categories. Further, they reinforce the statement that there is currently no sophisticated regulatory guidance (Bennett et al. 2020; Doan et al. 2021). Doan et al. (2021) conclude that NFTs have outpaced the existing regulatory and legal frameworks and that regulatory guidance is needed to ensure security. Subsequently, Bennett et al. (2020) conclude that there is a need for trust in blockchain technology which a fitting regulatory setting can achieve. They end their work with a call for a multi-stakeholder approach to DeFi standards and regulations. NFTs furthermore are in need of specially tailored laws that connect the transfer of off-chain assets and rights to the transfer of the on-chain token (Doan et al. 2021).

Suga et al. (2020) also acknowledge that there are re-centralized points and focus on crypto exchanges as such. They find that CEXs fulfill this point and connect off-chain with on-chain, while DEXs do not and thus will eliminate a point that regulation can grasp. They conclude that although there exist problems that are best solved by technology, there also is a need for thorough audits and sophisticated laws/standards; however, expertise in this field is currently lacking (which is in line with Bennett et al. (2020)). First, we thus find a commonly shared call for sophisticated DeFi laws that, on the one hand, account for its application in several jurisdictions and, on the other hand, includes all stakeholders of DeFi to obtain a generally accepted outcome. Second, it is a popular approach to propose re-centralized points in DeFi for regulations.

After having identified a need for regulation in certain aspects of DeFi, we want to turn to the literature that analyzes proposed regulations on DeFi in (2). There are two proposals for regulations analyzed, which are made by the Financial Crimes Enforcement Network (FinCEN) (Taylor 2021; Wright and Meier 2021) and the European Commission (Maia and Vieira dos Santos 2021). Under FinCEN's proposal, banks and money service businesses (MSBs) "would be required to submit reports, keep records, and verify the identity of customers participating in transactions above certain thresholds involving blockchain-based wallets not hosted by a financial institution […] or wallets hosted by a financial institution in certain jurisdictions identified by FinCEN" (Wright and Meier 2021). Wright and Meier (2021) proceed by analyzing comments on this proposal. It is found that the majority of DeFi institutions (e.g.: Coinbase, River Financial, Fidelity Digital Assets), blockchain developers, and other individuals are opposing this proposal. The main argument is that the proposal raises a heavy compliance burden on those banks and MSBs while not accounting for the features of DeFi and thus running the danger of not achieving its initial goal. The institutions highlight that this would increase the cost of service while decreasing user experience and would create incentives for users to switch to decentralized platforms that are harder to regulate (Wright and Meier 2021). Blockchain developers raise the concern that the blockchain was not intended to automatically collect user information, making such a regulation rather hard to attain technically, while individuals raise privacy concerns. Wright and Meier (2021) argue that the proposed data collection may deanonymize all transactions on a blockchain and thus arguably violates the fourth amendment and potentially further international privacy standards. They conclude that even if those concerns were to be solved, it remains an issue that users can switch to decentralized platforms that require an alternative approach to regulation which in turn may lead to a "hard-to-navigate patchwork of legal rules and regulations that would be inconsistent across different [protocols], companies and use cases (Wright and Meier 2021). The work of Taylor (2021) deals with anonymity-enhanced cryptocurrencies (AECs) that create an illicit finance threat in the eyes of FinCEN. FinCEN explicitly mentioned Dash as such currency and thus harmed this project as exchanges delisted the asset to comply with KYC and AML regulations (Taylor 2021). However, Taylor (2021) argues that Dash is not an AEC and mentions that despite efforts to contact FinCEN and pointing this out, FinCEN did not react and held on to its statement. We want to note that the author of (Taylor 2021) is, at the time of writing, CEO of the Dash Core Group.

While FinCEN's proposal mainly targets the jurisdiction of the USA, MiCA is a licensing regime across all EU member states (Maia and Vieira dos Santos 2021; Wright and Meier 2021). Maia and Vieira dos Santos (2021) summarize the goal of MiCA as follows: "MiCA has the purpose of providing legal certainty and instilling appropriate consumer and investor protection levels, financial stability, and market integrity to a growing, innovative and previously unregulated market without posing obstacles to the application of new technologies" (Maia and Vieira dos Santos 2021). MiCa also presents a categorization for crypto assets tied to regulatory consequences: crypto-assets can be either asset-referenced tokens (tokens which value refers to another asset), electronic money tokens (stablecoins), or other crypto assets. Utility tokens, however, are a sub-category of "other crypto assets" and qualify as securitization. Every service provider further needs authorization from a member state of the EU (Maia and Vieira dos Santos 2021). Maia and Vieira dos Santos (2021) highlight that MiCA does not explicitly refer to DeFi but find it helpful to analyze in which ways DeFi might be affected by it. They find that most DeFi services are not covered by MiCA as it is necessary to have a legal entity within an EU member state to comply with MiCA, and thus decentralized projects are not within the scope of this proposal. Maia and Vieira dos Santos (2021) conclude with suggestions on how to regulate these decentralized protocols and thus bridge the gap between (2) and (3). In line with the literature of (1), they find that "it is necessary to concede that a financial regulatory framework as we have today would not be enforceable to a decentralized protocol" (Maia and Vieira dos Santos 2021). They argue that regulation still is necessary, and that the regulatory entity's function should be prevention of DeFi risks such as cyber risks, frauds, manipulation, liquidity risk, etc., and providing advice on best practices in DeFi. Therefore, proper expertise must be ensured. They conclude that MiCA is a first step in the right direction and that a harmonized and international approach is the most promising, considering the border-less property of DeFi. We find that the existing regulatory approaches thus are not sophisticated DeFi laws but instead focus on financial assets or centralized aspects of DeFi without accounting for the decentralized aspect. Further, it seems that these regulatory approaches have multiple difficulties in their application to DeFi.

(3) The work of Hughes (2021) subsequently deals with the question of how effective regulation can be drafted. He starts by defining what effective regulation means in a DeFi context: ”(i) compliance with requirements such as registration of securities offerings, know-your-customer (KYC) rules, and the like, and (ii) attention to the contract and property rules integral to the enforceability of claims on assets” (Hughes 2021). It is raised again that compliance automation by integrating laws into code may be a promising and effective solution. However, he finds that developers have not yet accounted for property and bankruptcy laws. Hughes (2021) concludes that effective laws can only be drafted in a harmonized way by considering a multi-stakeholder approach. Matsuo (2020) and Takanashi (2020) both deal with such multi-stakeholder approaches. Takanashi (2020) present three regulatory goals: maintain financial stability, protect users, prevent financial crimes. He states that enforcement of existing rules becomes increasingly difficult, considering the properties of blockchains, and reinforces that integrating them in code might be the only way to accomplish the aforementioned goals. However, Takanashi (2020) acknowledges that this solution is of no value if nobody uses the platform that integrates such. Hence, he identifies the need for multi-stakeholder discussions to align interests and enable a healthy way to govern the DeFi ecosystem. Accomplishing a multi-stakeholder approach might be difficult since developers seem to embrace cypherpunk philosophy, meaning rejecting a central authority (Takanashi 2020).

Matsuo (2020) presents a first multi-stakeholder discussion on DeFi and identifies three aspects of a healthy DeFi system (permissionless innovation, global space, achieving regulatory goals) and the stakeholders of DeFi: engineers, businesses, regulators, and consumers. They are in line with Takanashi (2020), finding that developers often are reluctant to the idea of cooperating with regulators. Further, these stakeholders' pain points are mentioned: Businesses want to use the technology but face regulatory uncertainty, regulators lag behind on developments, consumers want transparency, but there is no authority to validate information on businesses. It was identified that there is a need for standardization and distribution of knowledge between the stakeholders. Some approaches to regulations were discussed, but it remained an open question on how to achieve regulatory goals in DeFi (Takanashi 2020). It is worthy to note that it was raised that “if an engineer decided to change the technology for the sake of regulation, it is a kind of suicide as an engineer in this community” (Takanashi 2020).

Contrary to that stands the work of Schrepel and Buterin (2020) that proposes blockchain code as a complementation to anti-trust laws. It is mentioned that "technology and law should be thought of allies - not enemies- because they feature complementary strengths" (Schrepel and Buterin 2020) and that despite the cypherpunk philosophy, blockchain's communities accept centralization, especially on a protocol level if a project turns out to be designed superiorly. Public blockchains are found to be ideal to complete antitrust because it decentralizes on a foundational level and anti-trust decentralizes to achieve its goal: competitive markets. However, turning regulatory power against the technology might endanger the whole blockchain ecosystem by destabilizing its internal governance mechanisms (Schrepel and Buterin 2020). They acknowledge that both developers and regulators might feel the need not to cooperate. However, they argue that it is the most dominant strategy for the common good to choose a cooperative approach since blockchains benefit from various legal protections and regulators can use a new technology to enforce laws. We want to highlight at this point that it is possible to detect unlawful behavior in DeFi automatically: Victor and Weintraud (2021) evaluated exchanges with regards to wash trading, which is thus a work at the intersection of law and technology, making use of both. However, they mention that there exists no sophisticated law on what constitutes as wash trading in DeFi.

4.3.3.2 DeFi Applications

Works in this category cover how governance and organization of DeFi protocols are facilitated. Considering the results of {Management & Organization | Users & Society}, we argue that an important question that should be addressed is how regulatory compliance can be implemented on a protocol level. We find that work in this category does not target this question but can be further split based on the objective of research into (1) DAOs and stablecoins (Brennecke et al. 2022; Klages-Mundt et al. 2020; Ushida and Angel 2021), (2) exchanges (Hickey and Harrigan 2021; Suga et al. 2020) and (3) various other protocols (Jensen et al. 2021; Nadler and Schär 2020; Perez et al. 2021).

(1) Ushida and Angel (2021) identify key factors that affect the governance of DeFi projects managed by DAOs. They find that while token governance seems to enjoy increasing popularity, it remains to be analyzed if this form of governance can be deemed appropriate for sustainable community development. A central concern is that governance token holders might prioritize short-term financial interest over the long-term stability of the project (Ushida and Angel

2021). In addition to the on-chain voting consensus, they identified an off-chain consensus process by the community where topics are discussed in forums. Ushida and Angel (2021) argue that a simple on-chain voting process might fail to account for the complex interplay of protocols by only favoring the protocol's governance token holders, while off-chain governance may be opaque and that the balance between transparency and security needs to be considered when designing governance mechanisms.

Brennecke et al. (2022) research MakerDAO, a DAO that manages the DAI stablecoin. They are in line with the findings of Ushida and Angel (2021) and find that an improvement of the governance in a system comes with an increase in value (value locked), while an increase in value requires the governance to run more efficiently. They conclude that currently, MakerDAO does not fully accomplish its management goals and could focus on aligning the protocol governance with regulatory policies. Gudgeon, Perez et al. (2020) are also concerned with the MakerDAO system and show the possibility of governance attacks against it. They show that it is possible to accumulate enough governance tokens to have the majority vote on a malicious executive contract that can steal funds locked as collateral. However, after disclosing this attack vector, MakerDAO adjusted its parameters so that a newly elected contract cannot be immediately executed (24h system time lock), giving time for participants to drop out in case of such an attack (Gudgeon, Perez et al. 2020). Klages-Mundt et al. (2020) cover the governance of stablecoins more generally and confirm previously mentioned results. They state that it can be expected that governance token holders maximize payoffs instead of focusing on system stability. They find that governance thus must be disincentivized from mismanagement and from opening up attack vectors (e.g.: by slashing governance token value).

It is often mentioned that the security of a protocol does not only concern the respective protocol governance but also the governance of other protocols that have a connection with that protocol (e.g.: oracles) and the underlying blockchain governance (e.g.: MEV and consensus) (Gudgeon, Perez et al. 2020; Klages-Mundt et al. 2020; Ushida and Angel 2021). Besides decentralized voting, it is possible that developers still hold admin keys to a protocol (Ushida and Angel 2021) and that there are stakeholders in a DAO project that have limited influence by not holding governance tokens (e.g.: operative actors and external actors) (Brennecke et al. 2022). Especially with non-custodial stablecoins, this seems to represent an issue since Klages-Mundt et al. (2020) find that incentive security for governance does not hold. Thus stablecoin holders (operative actors) may need to hold risky governance tokens to secure their stablecoin position against governance attacks, defeating the purpose of a stablecoin. Klages-Mundt et al. (2020)

conclude by drawing comparisons between stablecoin systems and lending pools / DEXs: they find that it might be easier to protect those since payout of governance attacks in comparison to fees are lower in DEXs and system time locks are more effective in lending pools.

This leads us to (2). Both works cover exchanges; however, Hickey and Harrigan (2021) are mainly concerned with a DEX (Bisq), while Suga et al. (2020) are concerned with CEXs. The work on Bisq deals with the privacy cost of participating in the Bisq DAO. Hickey and HarriganHickey and Harrigan (2021) identify mainly two categories of participants: Users and developers. Using the transparent bitcoin blockchain, Hickey and Harrigan (2021) employ an address clustering heuristic and find that it effectively aggregates all activities conducted by Bisq participants and that it is possible to attach real identities to many of its central participants. They state that, as decentralization pushes governments for more intrusive regulation, participants that can be identified may face increased regulatory burdens. Regarding countermeasures to this transparency and privacy dilemma, they find no solution that does not hinder application while increasing privacy (Hickey and Harrigan 2021).

Suga et al. (2020) present multiple issues of CEX that the Japanese financial services agency identified. They find that “there are no common understandings on the implementation and operations of financial services. The lack of management of system risks indicates that such cryptocurrency exchanges do not have enough number of qualified system architects, engineers, and operators” (Suga et al. 2020). Private key management is found to play an especially significant role in CEX governance. They argue that a CEX should manage a private key per customer instead of one private key per asset. They propose audits / external evaluations, multi-signature key schemes, and standardization of security management as further governance directions. In line with Klages-Mundt et al. (2020), Suga et al. (2020) acknowledge that CEXs operating on a segregated blockchain are potentially disadvantageous without further security measures.

(3) Perez et al. (2021) cover lending protocols and their governance mechanisms. It is found that governance tokens incentivize economic activity on these protocols; however, this is only sustainable if the price of the governance token is sufficiently high, which is in line with the findings of governance tokens and their incentive security in stablecoin systems (Klages-Mundt et al. 2020). A side effect of this is that users accept more risk, resulting in a higher risk of liquidations in collateralized lending protocols. Perez et al. (2021) also reinforce the previous

finding that risks stem from protocol dependencies and composability, as well as the underlying blockchain infrastructure that lies outside of the governance possibilities of a single protocol.

Jensen et al. (2021) and Nadler and Schär (2020) are concerned with governance tokens of various protocols. Both works find that governance tokens are concentrated among a small subset of addresses which raises questions regarding the decentralization property of protocols. More specifically, Jensen et al. (2021) analyze 4 prominent DeFi project governance tokens (BAL, COMP, UNI, YFI) and find that in each case, the top 100 addresses have a governance majority (51%) while Nadler and Schär (2020) analyze 18 governance tokens and find that in 15 cases the top 100 addresses have governance majority and that those top 500 addresses have the majority in all 18 cases. However, this does not directly mean that a DeFi application is prone to be vulnerable to governance attacks since security mechanisms (e.g.: time lock) vary from protocol to protocol but still carries implications when considering the governance design of DeFi protocols (Jensen et al. 2021; Nadler and Schär 2020).

4.3.3.3 Blockchain Infrastructure

Analogously to the previous category, this one deals with the governance of the blockchain infrastructure. Considering the previous findings especially in {Measurement & Value | DeFi Applications} and {Managements & Organization | DeFi Applications}, we argue that important topics to address are the transparency/security tradeoff and re-centralization issues regarding miners. We find that works currently do not address the aforementioned issues. It is unnecessary to split works in this category further since there are only four.

Schrepel and Buterin (2020) analyze the management of the blockchain infrastructure with regards to enabling decentralization. It is argued that if the blockchain is public and free to use, it facilitates decentralization by distributing control. As shown in {Management & Organization | DeFi Applications}, this theoretically enables the ability of the blockchain to complement antitrust law by facilitating a competitive market, although protocols may still be somewhat centralized (Schrepel and Buterin 2020).

Contrary to that stands the work of Aponte-Novoa et al. (2021), which find that the blockchain infrastructure may not be as decentralized as initially thought, but leaning towards heavy centralization of hashing power that represents a significant security risk. However, they conclude that while 51% attacks thus seem technically feasible, they are economically disincentivized and irrational since the credibility of the network and worth of its assets will plummet when successfully attacked. Subsequently, Qin, Zhou and Gervais (2021) show that miners, however, can extract value (if they possess enough hashing power) by using blockchain's transparency and their power to order transactions arbitrarily (see {Measurement & Value | DeFi Applications}). They further argue that this also endangers blockchain consensus security as miners may try to fork the blockchain to extract MEV. An additional problem on the blockchain infrastructure level is scalability (Zhao et al. 2021). Zhao et al. (2021) mention that the scalability of blockchains (transactions per second) is mainly determined by block generation time and block propagation delay. Block generation time must be consistently lower than block propagation delay since if blocks are created faster than nodes are receiving them, it can lead to consensus security issues (e.g.: forks) (Zhao et al. 2021). They argue that by decreasing propagation delay, block generation time can be decreased and proceed to propose their "LightBlock" protocol (see {Design & Features | Blockchain Infrastructure}).

4.3.3.4 Financial Industry

Management and organization deal with strategies and tactics employed by the financial industry concerning DeFi. It provides no additional value to split works in this category since there are only three items (all GL).

It was previously found in {Measurement & Value | Financial Industry} that advertising DeFi only based on highlighting shortcomings of traditional finance and referring to distrust in banks may not be the optimal way to approach DeFi adoption in the financial sector (Lockl and Stoetzer 2021). Lockl and Stoetzer (2021) propose that DeFi should be advertised by highlighting benefits over traditional services instead. All of the works in this category agree that traditional financial institutions do not feel threatened by the emergence of DeFi but rather see it as a welcome opportunity to make use of new technology (Derviz and others 2021; Lockl and Stoetzer 2021; Meegan and Koens 2021). Furthermore, they concur with the proposal of initiating a convergence of both financial systems. Such convergence is expected to propel users' benefits in the financial sector, for example, by integrating DeFi into existing product portfolios and legacy features (Derviz and others 2021; Lockl and Stoetzer 2021; Meegan and Koens 2021). As mentioned earlier, a promising point to initiate such a convergence is in stablecoins by CBDC (Derviz and others 2021). Meegan and Koens (2021) mention that as traditional financial businesses and institutions tend to be risk-averse, more work on DeFi is needed to reduce uncertainties and to help the traditional financial sector understand and engage with DeFi.

4.4 The current state of DeFi

Previously we analyzed findings of the DeFi literature in their respective categories and systematically summarized the existing body of knowledge. In the following, we want to analyze and discuss previous findings on a category-overarching level and draw prominent meta findings supported by a significant number of works.

First, we find that DeFi features mainly are transparency, composability, asset custody, privacy, atomicity of transactions, transaction order malleability, transaction fees, availability of services, anonymous development, decentralization, interoperability, borderlessness, and trustlessness. On the one hand, these properties are required for DeFi to fulfill its functions as a decentralized financial system (see: {Design & Features}, {Financial Industry}). On the other hand, those are also the features that may facilitate risks and disadvantages potentially leading to a financial system that is unstable, insecure, inefficient, and suffers from market manipulations and protocol attacks or enables various other illicit activities that can be conducted under the protection of a pseudonym (see: {Measurement & Value}). DeFi fulfills these features to different degrees, of which some even are in a trade-off (e.g.: privacy/transparency). The question to which degree what DeFi feature should be satisfied remains unanswered.

Second, we find that it is this dichotomy of DeFi that concerns regulators and lawmakers, leading to regulatory uncertainty. We find that the existing regulatory approaches are not sophisticated DeFi laws but instead focus on financial assets or centralized aspects of DeFi without accounting for the decentralized aspect. Further, it seems that these regulatory approaches have multiple difficulties in their application to DeFi. Especially decentralization and borderlessness prove to be intricate features of DeFi for regulatory approaches. There is thus a commonly shared call among the literature for sophisticated DeFi laws that, on the one hand, account for its properties (e.g.: application in several jurisdictions) and, on the other hand, considers all stakeholders of DeFi to obtain a generally accepted outcome (see: {Management & Organization | Users & Society}).

Third, we find that there seem to be multiple points of re-centralization in DeFi. Most prominently: oracles, reserve-backed stablecoins, governance tokens, hashing/validator power, and CEXs (see: {Design & Features}, {Measurement & Value}, {Management & Organization}). All of them fulfill a critical role in DeFi but introduce counterparty risk and single point of failures. There is a common approach to propose these re-centralized points in DeFi for regulatory actions and for initiating a convergence of CeFi and DeFi (e.g.: CBDCs as stablecoins) (see: {Management & Organization}).

Fourth, we find a risk that is often mentioned, yet little known about: dependencies (also often called systemic risk or contagion risk). It has two dimensions: (1) protocols being interconnected through their respective functions for each other in DeFi apps and (2) assets being interconnected by wrapping. A side effect of this interconnectedness is a significant increase in the complexity of the DeFi system (see {DeFi Applications}, {Blockchain Infrastructure}). It is expected that if an asset or protocol fails to fulfill its task, it could affect other parts of the financial system, potentially even leading to the downfall of the whole system in severe cases (see {Measurement & Value}). Known occasions are, for example, (1) oracle attacks that target one protocol to exploit another and (2) stablecoins deviate from their peg/collateral assets being volatile, sometimes resulting in liquidations of collateralized debt positions in various other protocols, potentially even leading to illiquidity spanning across all involved protocols of the "wrapping chain" in severe cases. Thus, we argue that wrapping processes in DeFi have similarities to the securitization process that opened up a systemic risk in the traditional financial system and led to the world financial crisis of 2008.

Fifth, there exist proposals for concepts, designs, and implementations that address some issues of DeFi. However, most of them are concerned with designing smart contracts to secure economic activity through economic incentives or technological code restraints. Generally, the security of DeFi applications can be split into incentive security and purely technological security by coded restraints (see {Design & Features}). We cannot make more specific statements on the effectiveness of proposed designs regarding identified problems since they lack thoroughly testing. However, we acknowledge that proposed solutions generally point towards some identified problems (see: {Design & Features}, {Measurement & Value}). Protocol dependencies and re-centralization in DeFi were not covered.

Sixth, we find that DeFi security is not only a matter of securing the respective protocols but also the underlying blockchain (see {DeFi Applications}, {Blockchain Infrastructure}). If the blockchain is not secure, the protocols are at risk, and potentially vice versa, as the implications of MEV on consensus security indicate (see {Design & Features}, {Measurement & Value}).

Seventh, we acknowledge a philosophical element inhering DeFi communities. Often in literature, it is referred to as cypherpunk philosophy, crypto-anarchism, or is captured by a definition of DeFi that represents the theoretical concept rather than its actual implementation. It is the very concept that ignited the spark for the creation of the first decentralized payment network (Bitcoin) and is deeply connected to distrust in state authority and traditional financial institutions, trying to decentralize and create a system where control and power are ultimately democratized among its participants (see {Measurement & Value}, {Management & Organization}). Persisting in that philosophy is found to hinder DeFi's adoption progress, especially regarding regulatory uncertainty and its integration into an institutionalized setting (traditional finance) (see {Management & Organization | Users & Society}, {Financial Industry}).

Eighth, generally, DeFi and CeFi are found to have similar goals: providing financial services to customers and do not contradict each other in their existence (see {Financial Industry}). However, both suffer from different respective weaknesses. It is thus commonly proposed that both systems learn from each other (e.g.: DeFi adopting well-established risk models of CeFi) (see: {Financial Industry}, {Users & Society}). Neither DeFi nor CeFi will likely replace the respective other in the future, but both systems will eventually co-exist, adopt methods from each other and converge.

Ninth, with regards to the current state of DeFi, the literature tends to agree that DeFi has not yet reached mainstream adoption as its risks are potentially high, markets are being inefficient, and the leading growth facilitator currently being high yields originating from complex wrapping operations (see {Measurement & Value}, {Management& Organization}). With maturing markets, increased security, and user adoption, it is expected that return on investments will converge with those of traditional financial markets, indicating that sustainable DeFi growth has to be based on other value propositions.

Remarkably, the entirety of work on blockchain features for DeFi does not identify smart contract functionality as a prerequisite for decentralized finance functionality (see {Design & Features | Blockchain Infrastructure}). We argue that DeFi thus also includes blockchains like Bitcoin, which are mainly for payment and do not possess sophisticated DeFi applications and protocols. However, the core of DeFi seems to be dominated by the Ethereum financial system and the financial services and instruments that can be found on it. Except for the mention of Facebook-Libra, we cannot find any indication that private or consortium blockchains play an important role for DeFi.

As we showed, there are currently multiple issues with DeFi, but as it has promising benefits for its users and especially those currently being unbanked or underbanked, it remains a highly relevant topic. Although it seems that some of DeFi's issues can be technically addressed, others seem to be more persistent and are possibly unable to be resolved that way, even in the distant future. We argue that especially the problem of re-centralization, the oracle problem, tying real-world assets to tokens, and illicit activities will prove hard to solve only by using code or technological advancements. We raise that it thus might be necessary for DeFi to work with regulators and lawmakers to formulate sophisticated DeFi laws that address these issues. However, there are (again) issues with implementing laws in DeFi, especially if users are reluctant to them. The only solution to approach this DeFi dilemma may thus be the multi-stakeholder approach that considers the needs of everyone.

Overall, we think that DeFi is yet not ready for mass adoption as it currently inhibits significant risks and is overall not very user-friendly. We see characterizations of DeFi range from being a financial system for criminal activities to an optimal tool to negate all the flaws of the traditional financial system and replace it. Considering the previously analyzed literature on DeFi, we argue that DeFi can never reach one of these extremes (i.e.: DeFi can never be fully decentralized, which also hinders its ability to become a financial system for criminal activities). Although its properties might enable its "dark side," they simultaneously enable its "benevolent side". Nevertheless, the state of DeFi can best be best described on a spectrum between those extremes: we argue that DeFi currently does not clearly tend towards one of those extremes, being located in an initial neutral position. We acknowledge that although DeFi has benevolent intentions, it needs external help and further research to overcome its issues and move towards a healthy and secure financial system that benefits the common good by offering distinct and sustainable financial services and goods.

The majority of works can be found in {Blockchain Infrastructure} and {DeFi Applications}, although works on DeFi applications vastly outnumber those on the blockchain infrastructure. We are confident that there is relevant research for DeFi regarding the foundational blockchain infrastructure that is not captured by our search string since those works may be purely blockchain orientated without connecting to DeFi. Nonetheless, the mere accumulation of works in both technological categories combined with the findings and the lack of works regarding business applications in the {Financial Industry} and {User & Society} categories suggest that DeFi is the result of a technology push. Hence, there is an urgent need to explore business and implementational use-cases.

Lastly, we want to highlight that in addition to the aforementioned point, existing works are predominantly concerned with the technology and its proper financial design. We argue that currently, development cooperation in DeFi mainly concerns the intersections of finance/economics and technology (as the categories {Measurement & Value | DeFi Applications} and {Measurement & Value | Blockchain Infrastructure} illustrate) while leaving out regulators and lawmakers. We want to connect this point to the finding of works in {Management & Organization | Users & Society}, often stating that there is a lack of knowledge regarding DeFi in regulatory approaches and that regulators lag behind, which is not surprising considering that regulatory practitioners do not seem to get involved in the development of DeFi.

5 Future research agenda

In the following, we reflect on identified issues and findings, thus setting out a research agenda containing the most pressing research opportunities and open questions regarding DeFi and its future development.

Table 4 shows the identified future research opportunities sorted into their respective categories; however, they are not isolated from other research opportunities. It is possible to cover multiple related questions in future works either by category (e.g.: {Design & Features | Users & Society}), level of analysis (e.g.:{Users & Society}) or activity (e.g.: {Design & Features}).

	Design & Features
Users & Society	▪ What are the required features for the user adoption of DeFi? ▪ What knowledge about DeFi, its concepts/features, and functions is needed for users to interact with it? ▪ What would make DeFi user-friendly/convenient?
DeFi Applications	▪ How can privacy technically be preserved although the need for transparency? ▪ How can DeFi applications be protected against vulnerabilities from interdependencies with other protocols? ▪ Can technology solve identified re-centralization issues? ▪ How can DeFi market inefficiencies be eased? ▪ How can the need for over-collateralization be eliminated? ▪ How should CBDCs as stablecoins be designed?
Blockchain Infrastructure	▪ How much transparency is technically needed? ▪ How can the scalability of blockchains be increased without jeopardizing security? ▪ How can extractable value attacks be technically prevented? ▪ Is transaction-order malleability a necessary DeFi feature, and can it be restricted to prevent MEV?

Financial Industry	▪ Is DeFi's transparency of use for audits, taxing, regulation, and reporting? ▪ What are the required features of DeFi for business use case adoption? ▪ What knowledge about DeFi, its concepts/features, and functions is needed for different businesses to integrate it into their business model?
	Measurement & Value
Users & Society	▪ Do users need DeFi (yet)? ▪ What are the value propositions of DeFi that are sustainable in the long run? ▪ Would DeFi communities accept a convergence of DeFi and CeFi? ▪ How distributed is knowledge about DeFi amongst different stakeholders? ▪ What is the general stance of the public towards DeFi?
DeFi Applications	▪ How effective are identified concepts in {Design & Features | DeFi}? ▪ Are flash loans a security threat for DeFi, and can their malicious use be limited? ▪ How and when is the process of wrapping assets threatening for DeFi? ▪ Could sophisticated DeFi laws improve application security and stability?
Blockchain Infrastructure	▪ How interconnected is DeFi across different platforms? ▪ Could private blockchain applications improve DeFi functionality? ▪ Could sophisticated DeFi laws improve infrastructural security and stability?
Financial Industry	▪ When is it rational to use DeFi over CeFi for finance use cases? ▪ What are potential DeFi use cases for businesses? ▪ Is DeFi a hedge against the traditional financial system? ▪ What are lessons learned from the development of the traditional financial system that can be applied to DeFi?
	Management & Organization
Users & Society	▪ How can regulators/lawmakers be included in the development of DeFi? ▪ Will it be possible to establish a multilateral and multi-stakeholder approach for DeFi regulation? ▪ Are regulators and lawmakers willing to adopt code as a form of "automated law" to some degree? ▪ How to manage the privacy/transparency trade-off?
DeFi Applications	▪ What DeFi laws are needed on a protocol/application level? ▪ How de(centralized) should the governance of a DeFi application be? ▪ Which financial laws should be designed as protocol codes? ▪ How can truly decentralized applications be regulated?
Blockchain Infrastructure	▪ What laws are needed on an infrastructural level? ▪ How de(centralized) should the governance of a blockchain for DeFi be? ▪ Which financial laws should be designed as blockchain code? ▪ How can an accumulation of validator power be prevented?
Financial Industry	▪ Which already existing financial laws are also applicable for DeFi businesses? ▪ Is it possible to regulate DeFi only by regulating centralized points of it? ▪ Are existing DeFi businesses effectively regulated? ▪ How can the convergence of DeFi and CeFi be initiated and fostered?

Table 5: Research agenda.
Source: Own illustration.

6 Conclusion

To the best of our knowledge, this is the first work that systematically analyses existing literature on decentralized finance. Our work is intended to provide a foundation for knowledge and further research on this topic. We summarized the existing body of knowledge using our established DeFi research framework and shed light on further research opportunities by establishing a DeFi research agenda that - we hope - may prove valuable to explore ways to foster the healthy development of DeFi.

The main limitations of this work stem from the selection process of the literature. While our search string ensured that we identified only relevant literature, we are confident that there are potentially relevant works for DeFi, which are not captured by it (e.g.: literature that only focuses on the infrastructural blockchain without mentioning DeFi). Further, we opted only to include grey literature of the highest tier of quality, resulting in the potential exclusion of relevant works. We covered the majority of academic databases for this topic, but the sources for grey literature were limited to GoogleScholar, RePEc, and arXiv.

We analyzed the literature on DeFi from different disciplines (Regulation, IT, and Finance) and have thus put together a puzzle of DeFi, illustrating an emerging financial ecosystem based on blockchain in dichotomy: theoretically and at best, it enables financial services in a truly decentralized financial system with its unique and democratizing concepts and features; and theoretically at worst, undermines the rule of law, enables illicit financial activity, and endangers everyone that puts funds in it. However, it seems that it is neither of both extremes at this current point in time and probably will never be able to reach one of those extremes in reality.

We frame the current implementation of DeFi as an emerging financial system that suffers from the very features that it draws its value propositions from. Further, it seems that DeFi will only overcome its issues by giving up on its initial philosophy of true decentralization and independence and by working together with regulators, lawmakers, and traditional financial institutions. It does not look like DeFi will ever fully replace traditional finance and its institutions; it is expected that both financial systems will need to converge to serve the most common good for users.

Therefore, we conclude that DeFi is currently not ready for mainstream adoption but may provide promising features and benefits for financial activities in the future, which makes research and improvements on DeFi a worthwhile endeavor. Further research on identified prevalent DeFi issues is greatly needed and will determine the general direction of DeFi.

We finish this work with a call for a multifaceted mindset. In our opinion, stakeholders of DeFi must detach themselves from an isolated view that is solely based on their needs and expectations of DeFi and consider the big picture of it that we have drawn. Considering the early state of DeFi, we advise generally keeping an open mind regarding further advancements, research, and propositions on DeFi, detaching from pre-set expectations of a silver bullet to issues of the traditional financial system or of a new inherently malicious financial system.

Bibliography

References

Adrian, T., & Shin, H. S. (2010). The Changing Nature of Financial Intermediation and the Financial Crisis of 2007–2009. *Annual Review of Economics, 2*(1), 603–618. doi:10.1146/annurev.economics.102308.124420

Amler, H., Eckey, L., Faust, S., Kaiser, M., Sandner, P., & Schlosser, B. (2021). *DeFi-ning DeFi: Challenges & Pathway*.

Angeris, G., & Chitra, T. (2020). Improved Price Oracles: Constant Function Market Makers. In : *AFT '20* (pp. 80–91). Association for Computing Machinery.

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,* 1. doi:10.1109/ACCESS.2021.3119291

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

Bahga, A., & Madisetti, V. K. (2020). A Value Token Transfer Protocol (VTTP) for Decentralized Finance. *Journal of Software Engineering and Applications, 13*(11), 303–311. doi:10.4236/jsea.2020.1311020

Barth, J., & Brumbaugh, R. (1997). Development and Evolution of National Financial Systems: An International Perspective.

Bartoletti, M., Chiang, J. H., & Lluch-Lafuente, A. (2021a). SoK: Lending Pools in Decentralized Finance. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Bartoletti, M., Chiang, J. H., & Lluch-Lafuente, A. (2021b). A Theory of Automated Market Makers in DeFi. In *Coordination Models and Languages* . Springer.

Bashir, M., Strickland, B., & Bohr, J. (2016). What Motivates People to Use Bitcoin? In *Spiro E., Ahn YY. (eds) Social Informatics. SocInfo 2016. Lecture Notes in Computer Science* .

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. doi:10.1111/1911-3838.12238

Brennecke, M., Guggenberger, T., Schellinger, B., & Urbach, N. (2022). The De-Central Bank in Decentralized Finance : A Case Study of MakerDAO. In

Brühl, V. (2020). Libra - A Differentiated View on Facebook's Virtual Currency Project. *Intereconomics, 55*(1), 54–61. doi:10.1007/s10272-020-0869-1

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110,* 102436. doi:10.1016/j.cose.2021.102436

Buterin, V. (2013). Ethereum white paper. Retrieved from https://ethereum.org/en/whitepaper/

Buterin, V. (2016). Ethereum: Platform Review. *Opportunities and Challenges for Private and Consortium Blockchains*.

Butijn, B.-J., Tamburri, D., & Heuvel, W.-J. (2019). Blockchains: a Systematic Multivocal Literature Review. doi:10.1145/3369052

Cadete de Matos, J., Fano, D., Lima, F., & Seneviratne, A. (2021). *The role of financial markets*. Retrieved 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-BASEL, 11*(16). doi:10.3390/app11167572

Caldarelli, G. (2020). Understanding the Blockchain Oracle Problem: A Call for Action. *Information, 11*(11), 509. doi:10.3390/info11110509

Cao, Y., Zou, C., & Cheng, X. (2021). *Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem*.

Carter, N., & Jeng, L. (2021). DeFi Protocol Risks: The Paradox of DeFi. *SSRN Electronic Journal*. doi:10.2139/ssrn.3866699

Castro, M., Liskov, B., & others (1999). Practical byzantine fault tolerance. In *OSDI* (Vol. 99, pp. 173–186).

Chanson, M., Martens, N., & Wortmann, F. (2020). THE ROLE OF USER-GENERATED CONTENT IN BLOCKCHAIN-BASED DECENTRALIZED FINANCE. *ECIS 2020 Proceedings*.

Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018). Blockchain and Scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122–128). IEEE.

Chen, Y., & Bellavitis, C. (2019). Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System. *SSRN Electronic Journal.* doi:10.2139/ssrn.3418557

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

Corbet, S., Goodell, J. W., Gunay, S., & Kaskaloglu, K. (2021). Are DeFi Tokens a Separate Asset Class from Conventional Cryptocurrencies? *SSRN Electronic Journal.* doi:10.2139/ssrn.3810599

Dai, W. (1998). *http://www.weidai.com/bmoney.txt*. Retrieved from http://www.weidai.com/bmoney.txt

Derviz, A., & others. (2021). Decentralised finance, its prospects and limits: Is blockchain interoperability the only obstacle? *Occasional Publications-Chapters in Edited Volumes,* 13–17.

Deutsche Bundesbank. (2019). *Money and Monetary Policy*. Retrieved from https://www.geld-und-geldpolitik.de/en/international-monetary-and-financial-system-chapter-7.html#nav-drei

Doan, A. P., Johnson, R. J., Rasmussen, M. W., Snyder, C. L., Sterling, J. B., & Yeargin, D. G. (2021). NFTs: Key U.S. Legal Considerations for an Emerging Asset Class. *Journal of Taxation of Investments, 38*(4), 63–68.

ECB. (1998). *Report on electronic money* (August 1998). Frankfurt am Main: Europ. Central Bank.

Fabozzi, F. J. (2008). Overview of Financial Instruments and Financial Markets. In F. J. Fabozzi (Ed.), *Handbook of Finance* . Hoboken, NJ, USA: John Wiley & Sons, Inc.

Galal, H. S., & Youssef, A. M. (2021). Publicly Verifiable and Secrecy Preserving Periodic Auctions. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2016). The need for multivocal literature reviews in software engineering. In S. Beecham, B. Kitchenham, & S. G. MacDonell (Eds.), *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering* (pp. 1–6). New York, NY, USA: ACM.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology, 106*, 101–121. doi:10.1016/j.infsof.2018.09.006

Gawlikowicz, W., Mannerings, B., Rudolph, T., & Šiška, D. (2021). Market Based Mechanisms for Incentivising Exchange Liquidity Provision. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Giles, R. P. (2008). The American Banking System. In F. J. Fabozzi (Ed.), *Handbook of Finance* . Hoboken, NJ, USA: John Wiley & Sons, Inc.

Grigo, J., Hansen, P., Patz, A., & Wachter, V. von. (2020). Decentralized Finance (DeFi)-A new Fintech Revolution. *The Blockchain Trend explained. Berlin: Bitkom*.

Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). The Decentralized Financial Crisis. In (pp. 1–15).

Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020). DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. In : *AFT '20* (pp. 92–112). Association for Computing Machinery.

Guseva, Y. (2021). The SEC, Digital Assets, and Game Theory. *Journal of Corporation Law, 46*(3), 629–679.

Han, R., Lin, H., & Yu, J. (2019). On the Optionality and Fairness of Atomic Swaps. In : *AFT '19* (pp. 62–75). Association for Computing Machinery.

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

Hughes, E. (1993). *A Cypherpunk's Manifesto*. Retrieved from https://www.activism.net/cypherpunk/manifesto.html

Hughes, H. (2021). Designing Effective Regulation for Blockchain-Based Markets. *Journal of Corporation Law, 46*(4), 899–908.

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. doi:10.1016/j.jisa.2021.102805

Irresberger, F., John, K., & Saleh, F. (2020). The Public Blockchain Ecosystem: An Empirical Analysis. *SSRN Electronic Journal.* doi:10.2139/ssrn.3592849

Jensen, J. R., Wachter, V. von, & Ross, O. (2021). *How Decentralized is the Governance of Blockchain-based Finance: Empirical Evidence from four Governance Token Distributions*.

Jones, D. M., & Rachlin, E. J. (2008). Monetary Policy: How the Fed Sets, Implements, and Measures Policy Choices. In F. J. Fabozzi (Ed.), *Handbook of Finance* . Hoboken, NJ, USA: John Wiley & Sons, Inc.

Kamei, F., Pinto, G., Wiese, I., Ribeiro, M., & Soares, S. (2021). What Evidence We Would Miss If We Do Not Use Grey Literature? In F. Lanubile (Ed.), *Proceedings of the 15th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)* (pp. 1–11). New York, NY, USA: ACM.

Katona, T. (2021). Decentralized Finance: The Possibilities of a Blockchain "Money Lego" System. *Financial and Economic Review, 20*(1), 74–102.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering, *2*.

Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y., & Minca, A. (2020). Stablecoins 2.0: Economic Foundations and Risk-Based Models. In : *AFT '20* (pp. 59–79). Association for Computing Machinery.

Kroon, H., Vos, M. de, & Pouwelse, J. (2021). Introducing Self-Sovereign Identity and Identity as Collateral in Decentralized Finance.

Kumar, M., Nikhil, N., & Singh, R. (2020). Decentralising Finance using Decentralised Blockchain Oracles. In (pp. 1–4).

Lerner, A. P. (1952). The Essential Properties of Interest and Money. *Quarterly Journal of Economics, 66*(2), 172. doi:10.2307/1882941

Li, J. (2021). DeFi as an Information Aggregator. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Li, J., Baldimtsi, F., Brandao, J. P., Kugler, M., Hulays, R., Showers, E., . . . Chang, J. (2021). Measuring Illicit Activity in DeFi: The Case of Ethereum. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Lipton, A., & Hardjono, T. (2021). Blockchain Intra-and Interoperability. *Innovative Technology at the Interface of Finance and Operations. Springer*.

Liu, Q., Yu, L., & Jia, C. (2020). MovER: Stabilize Decentralized Finance System with Practical Risk Management. In (pp. 55–56).

Lockl, J., & Stoetzer, J.-C. (2021). Trust-free Banking Missed the Point : The Effect of Distrust in Banks on the Adoption of Decentralized Finance. In

Maia, G., & Vieira dos Santos, J. (2021). MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). *SSRN Electronic Journal.* doi:10.2139/ssrn.3875355

Matsuo, S. (2020). Effectiveness of Multi-stakeholder Discussions for Decentralized Finance: A Conference Report of CoDeFi 2020. In *Financial Cryptography and Data Security* . Springer.

May, T. (1994). *The Crypto Anarchist Manifesto*. Retrieved from https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

McLeay, M., Radia, A., & Thomas, R. (2014). Money creation in the modern economy. *Bank of England Quarterly Bulletin*, Q1.

Meegan, X., & Koens, T. (2021). Lessons Learned from Decentralised Finance (DeFi). *ING. URL: https://new. ingwb. com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2. 0. pdf*.

Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. In G. Goos, J. Hartmanis, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, . . . C. Pomerance (Eds.), *Lecture Notes in Computer Science. Advances in Cryptology — CRYPTO '87* (pp. 369–378). Berlin, Heidelberg: Springer Berlin Heidelberg.

Nadler, M., & Schär, F. (2020). *Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution*.

Nakamoto, S. (2008). Bitcoin. *A peer-to-peer electronic cash system*.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. doi:10.1007/s12599-017-0467-3

Perez, D., Werner, S. M., Xu, J., & Livshits, B. (2021). Liquidations: DeFi on a Knife-Edge. In N. Borisov & C. Diaz (Eds.) (pp. 457–476). Springer Berlin Heidelberg.

Pourpouneh, M., Nielsen, K., & Ross, O. (2020). *Automated Market Makers*. Copenhagen.

Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, *59*(1), 69–76. doi:10.1007/s12599-017-0464-6

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). *CeFi vs. DeFi - Comparing Centralized to Decentralized Finance*.

Qin, K., Zhou, L., & Gervais, A. (2021). *Quantifying Blockchain Extractable Value: How dark is the forest?*

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework. *Business & Information Systems Engineering*, *59*(6), 385–409. doi:10.1007/s12599-017-0506-0

Rius, A., & Gashier, E. (2020). Smart Derivatives: On-Chain Forwards for Digital Assets. In *Leveraging Applications of Formal Methods, Verification and Validation: Applications* . Springer.

Rogaway, P., & Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, . . . W. Meier (Eds.), *Lecture Notes in Computer Science. Fast Software Encryption* (pp. 371–388). Berlin, Heidelberg: Springer Berlin Heidelberg.

Saengchote, K. (2021). Where do DeFi stablecoins go? A closer look at what DeFi composability really means. *SSRN Electronic Journal*. doi:10.2139/ssrn.3893487

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *FEDERAL RESERVE BANK OF ST LOUIS REVIEW*, *103*(2), 153–174. doi:10.20955/r.103.153-74

Schrepel, T., & Buterin, V. (2020). Blockchain Code as Antitrust. *SSRN Electronic Journal*. doi:10.2139/ssrn.3597399

Schueffel, P. (2017). Taming the Beast: A Scientific Definition of Fintech. *Journal of Innovation Management*, *4*(4). doi:10.24840/2183-0606_004.004_0004

Silberholz, J., & Di Wu, A. (2021). Measuring Utility and Speculation in Blockchain Tokens. *SSRN Electronic Journal*. doi:10.2139/ssrn.3915269

Smith, A. (1910). The Wealth of Nations. *Journal of Political Economy, 18*(5), 405. doi:10.1086/251711

Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing Cryptocurrency Exchange: Building up Standard from Huge Failures. In *Financial Cryptography and Data Security* . Springer.

Szabo, N. (1994). *Smart Contracts*. Retrieved from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT-winterschool2006/szabo.best.vwh.net/smart.contracts.html

Tai, S., Eberhardt, J., & Klems, M. (2017). Not ACID, not BASE, but SALT - A Transaction Processing Perspective on Blockchains. In *Proceedings of the 7th International Conference on Cloud Computing and Services Science* (pp. 755–764). SCITEPRESS - Science and Technology Publications.

Takanashi, Y. (2020). Future of Finance. In *Financial Cryptography and Data Security* . Springer.

Tapscott, A., & Tapscott, D. (2017). *How Blockchain Is Changing Finance*. Retrieved from https://hbr.org/2017/03/how-blockchain-is-changing-finance

Taylor, R. (2021). Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Tefagh, M., Bagheri, F., Khajehpour, A., & Abdi, M. (2020). Atomic Bonded Cross-Chain Debt. In : *ICBTA 2020* (pp. 50–54). Association for Computing Machinery.

Thakor, A. V. (1996). The design of financial systems: An overview. *Journal of Banking & Finance, 20*(5), 917–948. doi:10.1016/0378-4266(95)00033-X

Tien, S.-K., Wang, Y.-T., Cai, Y.-Z., & Tsai, M.-H. (2020). Maximizing the Time Value of Cryptocurrency in Smart Contracts with Decentralized Money Markets. In (pp. 503–508).

Tolmach, P., Li, Y., Lin, S.-W., & Liu, Y. (2021). Formal Analysis of Composable DeFi Protocols. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Ushida, R., & Angel, J. (2021). Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Varma, J. R. (2019). Blockchain in Finance. *Vikalpa: The Journal for Decision Makers, 44*(1), 1–11. doi:10.1177/0256090919839897

Venkatesh, Morris, & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425. doi:10.2307/30036540

Victor, F., & Weintraud, A. M. (2021). Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. In : *WWW '21* (pp. 23–32). Association for Computing Machinery.

Wachter, V., Jensen, J. R., & Ross, O. (2021). Measuring Asset Composability as a Proxy for DeFi Integration. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

Wang, B., Liu, H., Liu, C., Yang, Z., Ren, Q., Zheng, H., & Lei, H. (2021). BLOCKEYE: Hunting for DeFi Attacks on Blockchain. In (pp. 17–20).

Wang, Z., Jiang, G., & Ye, Q. (2021). On fair designs of cross-chain exchange for cryptocurrencies via Monte Carlo simulation. *Naval Research Logistics (NRL), n/a*(n/a). doi:10.1002/nav.21989

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii–xxiii. Retrieved from http://www.jstor.org/stable/4132319

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778*.

Wright, A., & Meier, S. (2021). Analyzing FinCEN's Proposed Regulation Relating to AML and KYC Laws. In *Financial Cryptography and Data Security. FC 2021 International Workshops* . Springer.

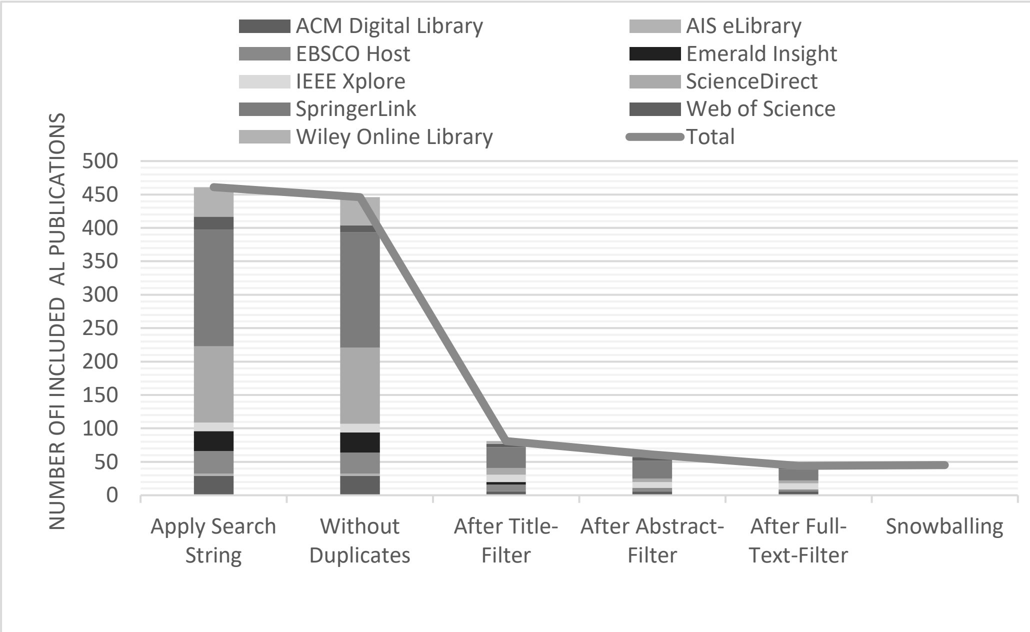
Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *JOURNAL OF FINANCIAL REGULATION*, *6*(2), 172–203. doi:10.1093/jfr/fjaa010

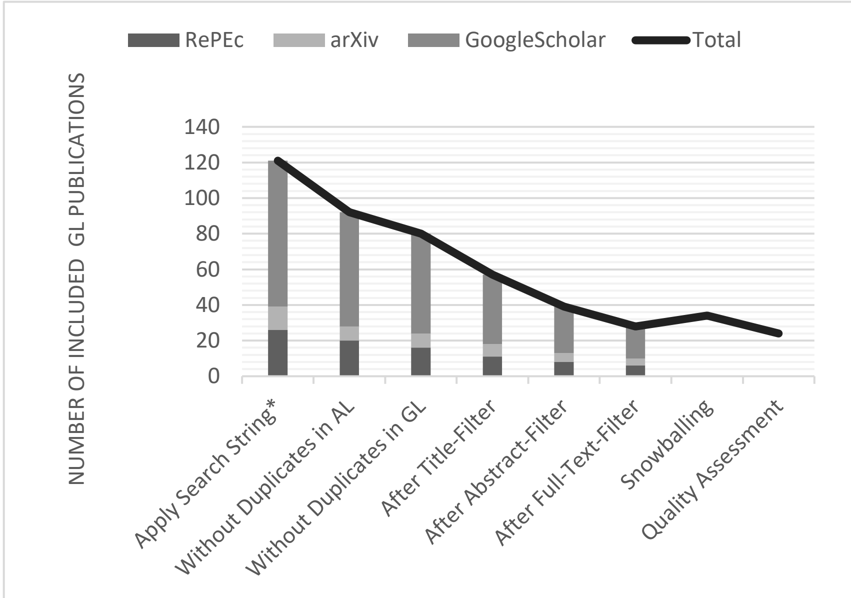
Zhao, C., Wang, T., & Zhang, S. (2021). LightBlock: Reducing Bandwidth Required to Synchronize Blocks in Ethereum Network. In (pp. 868–874).

Zhou, L., Qin, K., Cully, A., Livshits, B., & Gervais, A. (2021). On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols. In (pp. 919–936).

Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2021). High-Frequency Trading on Decentralized On-Chain Exchanges. In (pp. 428–445).

Appendix A.1. MLR search process illustrations.

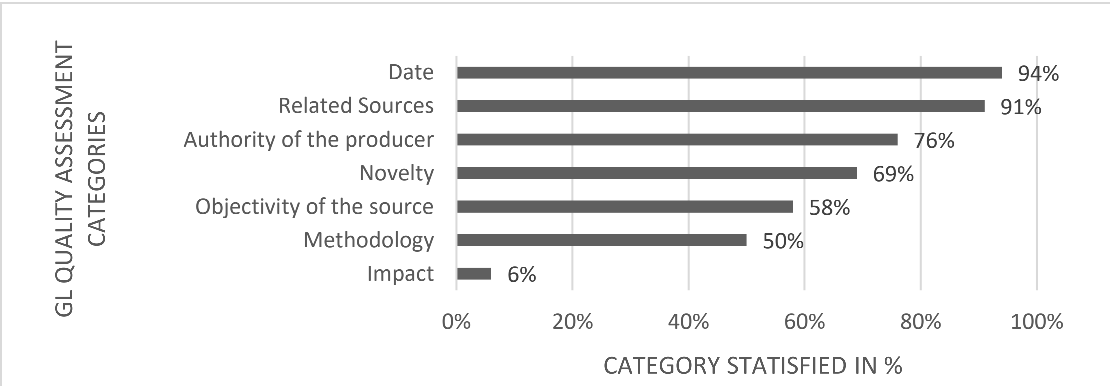




There is a sharp decline in AL in the Title-Filter, since a lot of items that fulfilled the search string with the combination of “DeFi” + “DLT” had nothing to do with Decentralized Finance. Example: “DeFi” was fulfiled by the word “Definition” and “DLT” was fulfilled as abbreviation for various other terms than distributed ledger technology, like “Double lung transplant”.

Appendix A.2. Grey literature quality assessment criteria.

Criteria Category	Quality Criteria
Authority of the producer	C1: The publishing organization is reputable, or the individual author is associated with a reputable organization
	C2: The author has published other work in the field
	C3: The author has expertise in the area (e.g. job title)
Objectivity of the source	C4: The statement of the sources is objective and the work is balanced in presentation
	C5: There are no vested interests
	C6: Conclusions are free of bias (e.g. supported by data)
Methodology	C7: The source has a clearly stated aim
	C8: The source has a clearly stated methodology
	C9: The source is supported by authoritative, documented references
	C10: Limits are clearly stated
	C11: The work covers a specific question
	C12: The work refers to a particular population or case
Date	C13: The item has a clearly stated date (does not have to be on the paper, but at least on the site refering to the paper)
Related Sources	C14: Key related GL or formal sources have been linked/discussed
Novelty	C15: The item enriches or adds something unique to the research
	C16: The item strengthens or refutes a current position
Impact	C17: The GL source should have citations and backlinks to substantiate the arguments made in the study (compact normalized metric)



Appendix B.1. Overview of the identified academic literature.

[#]	Title	Author (s)	Year	Publication venue
1	**A Theory of Automated Market Makers in DeFi**	Bartoletti, Massimo; Chiang, James Hsin-yu; Lluch-Lafuente, Alberto	2021	Conference Paper
2	**Analyzing FinCEN's Proposed Regulation Relating to AML and KYC Laws**	Wright, Aaron; Meier, Sachin	2021	Conference Paper
3	**Atomic Bonded Cross-Chain Debt**	Tefagh, Mojtaba; Bagheri, Fatemeh; Khajehpour, Amirhossein; Abdi, Melika	2020	Conference Paper
4	**Blockchain and Cryptoassets: Insights from Practice***	Bennett, Sheldon; Charbonneau, Ken; Leopold, Ryan; Mezon, Linda; Paradine, Carol; Scilipoti, Anthony; Villmann, Rebecca	2020	Journal Article
5	**Blockchain disruption and decentralized finance: The rise of decentralized business models**	Chen, Yan; Bellavitis, Cristiano	2020	Journal Article
6	**BLOCKEYE: Hunting for DeFi Attacks on Blockchain**	B. Wang; H. Liu; C. Liu; Z. Yang; Q. Ren; H. Zheng; H. Lei	2021	Conference Paper
7	**Decentralising Finance using Decentralised Blockchain Oracles**	M. Kumar; N. Nikhil; R. Singh	2020	Conference Paper
8	**Decentralized exchanges: The "wild west" of cryptocurrency trading**	Aspris, Angelo; Foley, Sean; Svec, Jiri; Wang, Leqi	2021	Journal Article
9	**Decentralized Finance**	Da Zetzsche; Arner, D. W.; Buckley, R. P.	2020	Journal Article
10	**Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets**	Schar, F.	2021	Journal Article
11	**DeFi as an Information Aggregator**	Li, Jiasun	2021	Conference Paper
12	**DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency**	Gudgeon, Lewis; Werner, Sam; Perez, Daniel; Knottenbelt, William J.	2020	Conference Paper
13	**Designing Effective Regulation for Blockchain-Based Markets**	Hughes, Heather	2020	Journal Article
14	**Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges**	Victor, Friedhelm; Weintraud, Andrea Marie	2021	Conference Paper

(continued on next page)

[#]	Title	Author (s)	Year	Publication venue
15	**Dynamic threshold ECDSA signature and application to asset custody in blockchain**	Wang, Huili; Ma, Wenping; Deng, Fuyang; Zheng, Haibin; Wu, Qianhong	2021	Journal Article
16	**Effectiveness of Multi-stakeholder Discussions for Decentralized Finance: A Conference Report of CoDeFi 2020**	Matsuo, Shin'ichiro	2020	Conference Paper
17	**Formal Analysis of Composable DeFi Protocols**	Tolmach, Palina; Li, Yi; Lin, Shang-Wei; Liu, Yang	2021	Conference Paper
18	**Future of Finance**	Takanashi, Yuta	2020	Conference Paper
19	**High-Frequency Trading on Decentralized On-Chain Exchanges**	L. Zhou; K. Qin; C. F. Torres; D. V. Le; A. Gervais	2021	Conference Paper
20	**Improved Price Oracles: Constant Function Market Makers**	Angeris, Guillermo; Chitra, Tarun	2020	Conference Paper
21	**Libra — A Differentiated View on Facebook's Virtual Currency Project**	Brühl, Volker	2020	Journal Article
22	**LightBlock: Reducing Bandwidth Required to Synchronize Blocks in Ethereum Network**	C. Zhao; T. Wang; S. Zhang	2021	Conference Paper
23	**Market Based Mechanisms for Incentivising Exchange Liquidity Provision**	Gawlikowicz, W.; Mannerings, B.; Rudolph, T.; Šiška, D.	2021	Conference Paper
24	**Maximizing the Time Value of Cryptocurrency in Smart Contracts with Decentralized Money Markets**	S. -K. Tien; Y. -T. Wang; Y. -Z. Cai; M. -H. Tsai	2020	Conference Paper
25	**Measuring Asset Composability as a Proxy for DeFi Integration**	Wachter, Victor; Jensen, Johannes Rude; Ross, Omri	2021	Conference Paper
26	**Measuring Illicit Activity in DeFi: The Case of Ethereum**	Li, Jiasun; Baldimtsi, Foteini; Brandao, Joao P.; Kugler, Maurice; Hulays, Rafeh; Showers, Eric; Ali, Zain; Chang, Joseph	2021	Conference Paper
27	**MovER: Stabilize Decentralized Finance System with Practical Risk Management**	Q. Liu; L. Yu; C. Jia	2020	Conference Paper
28	**NFTs: Key U.S. Legal Considerations for an Emerging Asset Class**	Doan, An P.; Johnson, Richard J.; Rasmussen, Mark W.; Snyder, Courtney Lyons; Sterling, Joshua B.; Yeargin, D. Grayson	2021	Journal Article
29	**On fair designs of cross-chain exchange for cryptocurrencies via Monte Carlo simulation**	Wang, Zini; Jiang, Guangxin; Ye, Qiang	2021	Journal Article

(continued on next page)

[#]	Title	Author (s)	Year	Publication venue
30	**On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols**	L. Zhou; K. Qin; A. Cully; B. Livshits; A. Gervais	2021	Conference Paper
31	**On the Optionality and Fairness of Atomic Swaps**	Han, Runchao; Lin, Haoyu; Yu, Jiangshan	2019	Conference Paper
32	**Publicly Verifiable and Secrecy Preserving Periodic Auctions**	Galal, Hisham S.; Youssef, Amr M.	2021	Conference Paper
33	**Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets**	Taylor, Ryan	2021	Conference Paper
34	**Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs**	Ushida, Ryosuke; Angel, James	2021	Conference Paper
35	**Securing Cryptocurrency Exchange: Building up Standard from Huge Failures**	Suga, Yuji; Shimaoka, Masaki; Sato, Masashi; Nakajima, Hirotaka	2020	Conference Paper
36	**Smart Derivatives: On-Chain Forwards for Digital Assets**	Rius, Alfonso D. D. M.; Gashier, Eamonn	2020	Conference Paper
37	**SoK: Lending Pools in Decentralized Finance**	Bartoletti, Massimo; Chiang, James Hsin-yu; Lafuente, Alberto Lluch	2021	Conference Paper
38	**Stablecoins 2.0: Economic Foundations and Risk-Based Models**	Klages-Mundt, Ariah; Harz, Dominik; Gudgeon, Lewis; Liu, Jun-You; Minca, Andreea	2020	Conference Paper
39	**The 51% Attack on Blockchains: A Mining Behavior Study**	F. A. Aponte-Novoa; A. L. S. Orozco; R. Villanueva-Polanco; P. Wightman	2021	Journal Article
40	**The Bisq decentralised exchange: On the privacy cost of participation**	Hickey, Liam; Harrigan, Martin	2021	Journal Article
41	**The Blockchain Oracle Problem in Decentralized Finance-A Multivocal Approach**	Caldarelli, G.; Ellul, J.	2021	Journal Article
42	**The De-Central Bank in Decentralized Finance: A Case Study of MakerDAO**	Brennecke, Martin; Guggenberger, Tobias; Schellinger, Benjamin; Urbach, Nils	2021	Conference Paper
43	**The Decentralized Financial Crisis**	L. Gudgeon; D. Perez; D. Harz; B. Livshits; A. Gervais	2020	Conference Paper
44	**The SEC, Digital Assets, and Game Theory**	Guseva, Yuliya	2020	Journal Article
45	**What Motivates People to Use Bitcoin?**	Bashir, Masooda; Strickland, Beth; Bohr, Jeremiah	2016	Conference Paper

Appendix B.2. Overview of the identified grey literature.

[#]	Title	Author (s)	Year	Publication venue
46	**A Value Token Transfer Protocol (VTTP) for Decentralized Finance**	Bahga, Arshdeep; Madisetti, Vijay K.	2020	Eprint
47	**Are DeFi Tokens a Separate Asset Class from Conventional Cryptocurrencies?**	Corbet, Shaen; Goodell, John W.; Gunay, Samet; Kaskaloglu, Kerem	2021	Technical Report
48	**Automated Market Makers**	Pourpouneh, Mohsen; Nielsen, Kurt; Omri, Ross	2020	Working Paper
49	**Blockchain Code as Antitrust**	Schrepel, Thibault; Buterin, Vitalik	2020	Technical Report
50	**Blockchain Intra- and Interoperability**	Lipton, A.; Hardjono, T.	2020	Preprint
51	**CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance**	Qin, Kaihua; Zhou, Liyi; Afonin, Yaroslav; Lazzaretti, Ludovico; Gervais, Arthur	2021	Technical Report
52	**Decentralized Finance - The Possibilities of a Blockchain "Money Lego" System**	Katona, Tamás	2021	Whitepaper
53	**Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution**	Nadler, Matthias; Schär, Fabian	2020	Technical Report
54	**Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System**	Chen, Yan	2019	Technical Report
55	**DeFi Protocol Risks: The Paradox of DeFi**	Carrter, Nic; Jeng, Linda	2021	Preprint
56	**DeFi-ning DeFi: Challenges & Pathway**	Amler, Hendrik; Eckey, Lisa; Faust, Sebastian; Kaiser, Marcel; Sandner, Philipp; Schlosser, Benjamin	2021	Technical Report
57	**Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem**	Cao, Yixin; Zou, Chuanwei; Cheng, Xianfeng	2021	Technical Report
58	**Global Economic Outlook_ July 2021 / Decentralised finance, its prospects and limits: Is blockchain interoperability the only obstacle?**	Czech National Bank	2021	Whitepaper

(continued on next page)

[#]	Title	Author (s)	Year	Publication venue
59	**How Decentralized is the Governance of Blockchain-based Finance_ Empirical Evidence from four Governance Token Distributions**	Rude Jensen, Johannes; von Wachter, Victor; Ross, Omri	2021	Working Paper
60	**Introducing_Self_Sovereign_Identity_and_Identity_as_Collateral_in_Decentralized_Finance**	Kroon, Harmen; de Vos, Martijn; Pouwelse, Johan	2021	Eprint
61	**Lessons Learned from Decentralised Finance (DeFi)**	Meegan, X.; Koens, T.	2021	Whitepaper
62	**Liquidations: DeFi on a Knife-edge**	Perez, Daniel; Werner, Sam M.; Xu, Jiahua; Livshits, Benjamin	2020	Preprint
63	**Measuring Utility and Speculation in Blockchain Tokens**	Silberholz, John; Wu, Di (Andrew)	2021	Technical Report
64	**MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance')**	Maia, Guilherme; Vieira dos Santos, João	2021	Preprint
65	**Quantifying Blockchain Extractable Value: How dark is the forest?**	Qin, Kaihua; Zhou, Liyi; Gervais, Arthur	2021	Technical Report
66	**The Public Blockchain Ecosystem: An Empirical Analysis**	Irresberger, Felix; John, Kose; Saleh, Fahad	2020	Technical Report
67	**THE ROLE OF USER-GENERATED CONTENT IN BLOCKCHAIN-BASED DECENTRALIZED FINANCE**	Mathieu Chanson, Nils Martens, and Felix Wortmann	2020	Eprint
68	**TRUST-FREE BANKING MISSED THE POINT – THE EFFECT OF DISTRUST IN BANKS ON THE ADOPTION OF DECENTRALIZED FINANCE**	Lockl, Jannik; Stoetzer, Jens-Christian	2021	Eprint
69	**Where do DeFi stablecoins go? A closer look at what DeFi composability really means**	Saengchote, Kanis	2021	Technical Report

Appendix C.1. Classification of the identified literature into our framework.

	Design & Features	Measurement & Value	Management & Organization
Users & Society	(Chen and Bellavitis 2020) (Aspris et al. 2021) (Bashir et al. 2016) (Irresberger et al. 2020) (Chanson et al. 2020) (Lockl and Stoetzer 2021)	(Bennett et al. 2020) (Chen and Bellavitis 2020) (Schär 2021) (Tolmach et al. 2021) (Qin, Zhou, Afonin et al. 2021) (Katona 2021) (Carter and Jeng 2021) (Amler et al. 2021)	(Wright and Meier 2021) (Bennett et al. 2020) (Zetzsche et al. 2020) (Hughes 2021) (Victor and Weintraud 2021) (Matsuo 2020) (Takanashi 2020) (Doan et al. 2021) (Taylor 2021) (Ushida and Angel 2021) (Suga et al. 2020) (Guseva 2021) (Schrepel and Buterin 2020) (Qin, Zhou, Afonin et al. 2021) (Maia and Vieira dos Santos 2021)

(continued on next page)

	Design & Features	Measurement & Value	Management & Organization
DeFi Applications	(Bartoletti et al. 2021b) (Kumar et al. 2020) (Zhou, Qin, Torres et al. 2021) (Angeris and Chitra 2020) (Gawlikowicz et al. 2021) (Tien et al. 2020) (Galal and Youssef 2021) (Rius and Gashier 2020) (Bartoletti et al. 2021a) (Bahga and Madisetti 2020) (Pourpouneh et al. 2020) (Lipton and Hardjono 2021) (Kroon et al. 2021)	(Wang, B. et al. 2021) (Aspris et al. 2021) (Schär 2021) (Li 2021) (Gudgeon, Werner et al. 2020) (Victor and Weintraud 2021) (Huili et al. 2021) (Zhou, Qin, Torres et al. 2021) (Angeris and Chitra 2020) (Wachter et al. 2021) (Liu et al. 2020) (Zhou, Qin, Cully et al. 2021) (Bartoletti et al. 2021a) (Klages-Mundt et al. 2020) (Caldarelli and Ellul 2021) (Brennecke et al. 2022) (Gudgeon, Perez et al. 2020) (Corbet et al. 2021) (Pourpouneh et al. 2020) (Nadler and Schär 2020) (Carter and Jeng 2021) (Amler et al. 2021) (Cao et al. 2021) (Jensen et al. 2021) (Perez et al. 2021) (Silberholz and Di Wu 2021) (Saengchote 2021)	(Ushida and Angel 2021) (Suga et al. 2020) (Klages-Mundt et al. 2020) (Hickey and Harrigan 2021) (Brennecke et al. 2022) (Gudgeon, Perez et al. 2020) (Nadler and Schär 2020) (Jensen et al. 2021) (Perez et al. 2021)

(continued on next page)

	Design & Features	Measurement & Value	Management & Organization
Blockchain Infrastructure	(Tefagh et al. 2020) (Huili et al. 2021) (Zhou, Qin, Torres et al. 2021) (Brühl 2020) (Zhao et al. 2021) (Li et al. 2021) (Han et al. 2019) (Galal and Youssef 2021) (Aponte-Novoa et al. 2021) (Lipton and Hardjono 2021) (Qin, Zhou, Afonin et al. 2021) (Chen and Bellavitis 2019) (Amler et al. 2021) (Qin, Zhou and Gervais 2021)	(Wang, Z. et al. 2021) (Han et al. 2019) (Bahga and Madisetti 2020) (Lipton and Hardjono 2021) (Carter and Jeng 2021) (Irresberger et al. 2020)	(Zhao et al. 2021) (Aponte-Novoa et al. 2021) (Schrepel and Buterin 2020) (Qin, Zhou and Gervais 2021)
Financial Industry	(Chen and Bellavitis 2020) (Qin, Zhou, Afonin et al. 2021) (Katona 2021) (Chen and Bellavitis 2019) (Derviz and others 2021) (Meegan and Koens 2021)	(Chen and Bellavitis 2020) (Kumar et al. 2020) (Schär 2021) (Qin, Zhou, Afonin et al. 2021) (Katona 2021) (Derviz and others 2021) (Meegan and Koens 2021) (Lockl and Stoetzer 2021)	(Derviz and others 2021) (Meegan and Koens 2021) (Lockl and Stoetzer 2021)

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten Schriften entnommen wurden, sind als solche gekennzeichnet.

Die Arbeit hat in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen.

Bayreuth, den 10. Januar 2022

(Marc Principato)

Statutory Declaration

I hereby declare that I have prepared this work independently and without the use of any other aids than those indicated. All passages that have been taken verbatim or in spirit from published writings are marked as such.

The thesis has not been submitted in the same or similar form to any other examination authority.

Bayreuth, 10. January 2022

(Marc Principato)