DISCUSSION PAPER SERIES

DP18038

THE TECHNOLOGY OF DECENTRALIZED FINANCE (DEFI)

Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese and Victor Friedhelm

INDUSTRIAL ORGANIZATION, INTERNATIONAL MACROECONOMICS AND FINANCE AND BANKING AND CORPORATE FINANCE

ISSN 0265-8003

THE TECHNOLOGY OF DECENTRALIZED FINANCE (DEFI)

Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese and Victor Friedhelm

Discussion Paper DP18038
Published 29 March 2023
Submitted 23 February 2023

Centre for Economic Policy Research
33 Great Sutton Street, London EC1V 0DX, UK
Tel: +44 (0)20 7183 8801
www.cepr.org

THE TECHNOLOGY OF DECENTRALIZED FINANCE (DEFI)

Abstract

Decentralized Finance (DeFi) is a new financial paradigm that leverages distributed ledger technologies to offer services such as lending, investing, or exchanging cryptoassets without relying on a traditional centralized intermediary. A range of DeFi protocols implements these services as a suite of smart contracts, ie software programs that encode the logic of conventional financial operations. Instead of transacting with a counterparty, DeFi users thus interact with software programs that pool the resources of other DeFi users to maintain control over their funds. This paper provides a deep dive into the overall architecture, the technical primitives, and the financial functionalities of DeFi protocols. We analyse and explain the individual components and how they interact through the lens of a DeFi stack reference (DSR) model featuring three layers: settlement, applications and interfaces. We discuss the technical aspects of each layer of the DSR model. Then, we describe the financial services for the most relevant DeFi categories, ie decentralized exchanges, lending protocols, derivatives protocols and aggregators. The latter exploit the property that smart contracts can be “composed”, ie utilize the functionalities of other protocols to provide novel financial services. We discuss how composability allows complex financial products to be assembled, which could have applications in the traditional financial industry. We discuss potential sources of systemic risk and conclude by mapping out an agenda for research in this area.

JEL Classification: E42, E58, F31, G19, G23, L50, O33, G12

Keywords: Blockchain, Ethereum, Cryptocurrencies, Stablecoins

Raphael Auer - raphael.auer@gmail.com
Bank For International Settlements and CEPR

Bernhard Haslhofer - haslhofer@csh.ac.at
Complexity Science Hub Vienna

Stefan Kitzler - kitzler@csh.ac.at
Complexity Science Hub, Vienna and AIT - Austrian Institute of Technology

Pietro Saggese - saggese@csh.ac.at
Complexity Science Hub, Vienna and AIT - Austrian Institute of Technology

Victor Friedhelm - friedhelm.victor@tu-berlin.de
Technische Universität Berlin (TU Berlin)

Acknowledgements
The views expressed in this document are those of the authors and not necessarily the views of the BIS. We thank Matteo Aquilina, Rainer Böhme, Andrea Canidio, Emma Claggett, Christian Diem, Nicola Dimitri, Alexander Eisl, Pirmin Fessler, Jon Frost, Arthur Gervais, Aljosha Judmayer, Masarah Paquet-Clouston, Krzysztof Paruch, Burkhard Raunig, Andreas Schrimpf, Esther Segalla, Nicholas Stifter, Martin Summer, Stefan Thurner, Marcus Wunsch, and Teng Andrea Xu.

The Technology of Decentralized Finance (DeFi)

Raphael Auer* Bernhard Haslhofer† Stefan Kitzler‡ Pietro Saggese§
Friedhelm Victor¶

January 26, 2023

Abstract

Decentralized Finance (DeFi) is a new financial paradigm that leverages distributed ledger technologies to offer services such as lending, investing, or exchanging cryptoassets without relying on a traditional centralized intermediary. A range of DeFi protocols implements these services as a suite of smart contracts, ie software programs that encode the logic of conventional financial operations. Instead of transacting with a counterparty, DeFi users thus interact with software programs that pool the resources of other DeFi users to maintain control over their funds. This paper provides a deep dive into the overall architecture, the technical primitives, and the financial functionalities of DeFi protocols. We analyse and explain the individual components and how they interact through the lens of a DeFi stack reference (DSR) model featuring three layers: settlement, applications and interfaces. We discuss the technical aspects of each layer of the DSR model. Then, we describe the financial services for the most relevant DeFi categories, ie decentralized exchanges, lending protocols, derivatives protocols and aggregators. The latter exploit the property that smart contracts can be "composed", ie utilize the functionalities of other protocols to provide novel financial services. We discuss how composability allows complex financial products to be assembled, which could have applications in the traditional financial industry. We discuss potential sources of systemic risk and conclude by mapping out an agenda for research in this area.

Keywords: Financial engineering, Decentralized Finance, DeFi, Blockchain, Ethereum, DLT, Cryptocurrencies, Stablecoins, Cryptoassets

JEL classification: E42, E58, F31, G19, G23, L50, O33, G12

*Bank for International Settlements; email: raphael.auer@bis.org. The views expressed in this document are those of the authors and not necessarily the views of the BIS. †Complexity Science Hub Vienna; email: haslhofer@csh.ac.at. ‡,§Complexity Science Hub Vienna and AIT — Austrian Institute of Technology; email: kitzler@csh.ac.at and saggese@csh.ac.at. ¶Technische Universität Berlin; email: friedhelm.victor@tu-berlin.de. We thank Matteo Aquilina, Rainer Böhme, Andrea Canidio, Emma Claggett, Christian Diem, Nicola Dimitri, Alexander Eisl, Pirmin Fessler, Jon Frost, Arthur Gervais, Aljosha Judmayer, Masarah Paquet-Clouston, Krzysztof Paruch, Burkhard Raunig, Andreas Schrimpf, Esther Segalla, Nicholas Stifter, Martin Summer, Stefan Thurner, Marcus Wunsch, and Teng Andrea Xu.

1 Introduction

Decentralized Finance (DeFi) offers on-chain financial services such as borrowing, lending, or investing without relying on a traditional centralized financial intermediary [121]. DeFi applications strive for disintermediation and censorship resistance, with partial success [32, 42, 133]. They are often realized as open-source software and enable governance models that let arbitrary stakeholders participate in decision-making processes [66]. Technically, such services are implemented as executable software programs called *smart contracts* whose execution is automated, ensuring deterministic outcomes and re-usability. These programs are then deployed on smart contract-enabling distributed ledger technologies (DLTs) such as Ethereum [124] or Tron. Interest in DeFi rose sharply in 2020 and, during its peak in 2021, reached a total value locked (TVL) of more than 150 billion USD [40].[1]

It is still unclear if and to what extent DeFi will proliferate in the future [23]. Today even most cryptocurrency trading happens off-chain on centralized crypto exchanges, which does not constitute DeFi [13, 10]. Recent episodes of market turmoil have led to a discussion on whether and how the DeFi industry should be regulated [109, 8].

Nevertheless, we consider DeFi a relevant development because it harnesses innovative technology that might shape the future financial ecosystem. This innovation can be traced back to the following three fundamental characteristics, which are of interest well beyond cryptocurrency markets. First is the algorithmic automation of financial activity, such as market-making, supporting the pooling of assets of small and large-scale actors alike. In the best case, such algorithmic services might reduce inefficiencies while being transparent to all parties, also allowing users to retain full control over their funds [61].

Second is enabling a novel form of competitive financial engineering, reinforced by what are known as "DeFi compositions" where financial service providers can combine the financial functions of several DeFi protocols to offer novel, complex, and deeply nested financial products without being dependent on any single intermediary [71]. This is possible because DeFi protocols are, in essence, computer programs that can automatically call on other computer programs.

Third, and related to the previous aspects, DeFi could be a blueprint of how technology can enable new forms of openness to the financial sector. One could envision making use of the underlying technology in the current financial system to provide stability and scale for programmable finance ecosystems [23].[2]

However, DeFi introduces enormous technological and economic complexity that makes the interpretation, evaluation, and risk assessment of DeFi financial products increasingly difficult. A systematic evaluation of these aspects is needed by financial institutions and regulators dealing with DeFi (e.g., [57, 10]). Recent research has shown how DeFi is subject to risks common to the broader financial system: lending protocols can become insufficiently collateralized or insolvent [59]. Furthermore, the promises of transparency and stability in DeFi are not necessarily guaranteed, as is exemplified by investigations into the Tether stablecoin [26]. A stablecoin run with consequent deleveraging spiral effects [25, 74] involved Terra's algorithmic stablecoin protocol and its associated cryptoassets, LUNA and UST, leading to its rapid collapse. The UST stablecoin was exploited in many DeFi protocols built on the Terra blockchain and through bridges on different blockchains. Its crash affected large parts of the DeFi ecosystem [100]. Furthermore, miners and validators can choose which transactions they add to the ledger and

[1] TVL has emerged as a popular indicator to quantify and measure the performance of a DeFi protocol. It is generally defined as the total value of cryptoassets locked in a protocol by users. Technically, TVL for a given DeFi protocol is computed by retrieving and pricing token balances from associated smart contacts. The decision of which assets of a given DeFi protocol to include in calculating the TVL value does not follow a standardized procedure. As a result, it can lead to different interpretations and even manipulation (cf. [90, 89]).

[2] One example in this direction is Project Mariana of the BIS Innovation Hub, the Eurosystem's Banque de France, the Monetary Authority of Singapore, and the Swiss National Bank, which examines the role of automated market-makers in foreign exchange markets [24].

in which order, giving rise to the prevalence of front-running, sandwich trades, and related issues [14]. The rise of DeFi has been accompanied by many incidents with an accumulated total loss exceeding 3 billion USD [133]. These incidents highlight the risks of technical vulnerabilities [34] and their amplification caused by the intertwined nature of DeFi protocols [71].

A deep understanding of DeFi is still lacking in many circles, which calls for a specific framework for an improved working knowledge of the technology. Therefore, in this paper, we introduce the technical fundamentals and financial functions of DeFi to a broad audience having diverse backgrounds. In addition, we include the most recent findings and advancements that contribute to understanding their functioning, design, and how they can interoperate.

Building on previous work [34, 121, 107, 133], we start by introducing the DeFi Stack Reference (DSR) model in Section 2 as a conceptualization of the technical primitives and financial functions that DeFi protocols build upon. Then, in Section 3, we describe in more detail the essential technical primitives, such as DLTs and smart contracts. Next, in Section 4, we outline the spectrum of cryptoassets used to represent and transfer value in the DeFi ecosystem. In Section 5, we describe the design and financial functions of the most prominent DeFi protocol families and abstract them into a generalized DeFi framework. After explaining the core components and functions of individual DeFi protocols, we describe how they can be combined into DeFi compositions (Section 6). Finally, in Section 7, we outline an interdisciplinary agenda that follows the DSR model and indicates future research directions.

2 DeFi Definition and Stack Reference (DSR) Model

We start by providing a high-level definition of DeFi before we introduce the DSR Model.

Definition 1 ***Decentralized Finance (DeFi) is a competitive, contestable, composable and non-custodial financial ecosystem built on technology that does not require a central organization to operate and that has no safety net.*** *It consists of financial protocols — implemented as "smart contracts" — running on a network of computers to automatically manage financial transactions. Implemented on top of DLT, it does not require banks or other traditional centralized intermediaries. The underlying ecosystem is competitive as novel intermediaries — miners or validators — compete to process and settle transactions. Users can choose from different financial protocols; these are contestable as anyone can become an intermediary or deploy a protocol or even start a new ledger; composable as complex services can be assembled from basic protocols; and non-custodial as users can keep direct custody of their assets when accessing financial services. DeFi does not come with any safety net as it lacks protection from criminal conduct or investor fraud and erroneous transactions cannot be undone.*

We note that DeFi is larger than an individual cryptocurrency such as Ethereum. Instead, the overall DeFi ecosystem appears as a composite and somewhat fragmented collection of individual subsystems, each built on top of one DLT with specific technical features that delineate and delimit the design choices of the financial protocols that can be implemented on it. This could change in the future, as several projects currently try to implement communication channels across DLTs. At the time of writing, Ethereum represents the most relevant DeFi subecosystem, both in terms of value locked and relevance of financial protocols built on top of it.

We also note that only "on-chain"[3] financial activity can be categorized as DeFi. Cryptoasset exchanges such as the recently collapsed FTX,[4] are primarily centralized platforms that provide interfaces to buy and sell cryptoassets using conventional IT systems. They manage and match orders in a private limit order book, with no direct effect on the DLT. Similarly, cryptoasset

[3] We use the term "on-chain" loosely to denote transactions executed and recorded on a distributed ledger.

[4] See `https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d` on the FTX failure.

loan companies like Celsius[5] act as a centralized intermediary. Customers that interact with such platforms or with conventional institutions give up custody of their assets.

Instead, DeFi aims at disintermediation: users interact with smart contracts, rather than with an institution, and no user identification is required. As an example, lending in DeFi is facilitated by smart contracts that hold the cryptoassets deposited by the lenders, that in turn can be borrowed by other DeFi users who are also interacting with a smart contract.

The exchange of cryptoassets in DeFi is executed in a similar fashion: while some users can provide liquidity by depositing funds in smart contracts, others can exchange them directly against the contract, and prices are updated automatically. These financial services are not controlled and supervised by traditional financial institutions or market authorities, ie they do not come with safeguards against criminal activity or investor fraud.

DeFi protocols implement such financial services as a suite of smart contracts. As any other modern software program, they also follow the "abstraction principle", which encapsulates well-defined functions in multiple abstraction layers, each using functionality provided by the one immediately beneath and offers functionality to the one above. In earlier research, Schär introduced a layered framework for DeFi [107]. Building on this and other related DeFi stack approaches [34, 121], considering new developments in the literature, as well as expanding the concept of composability in DeFi, we introduce a DeFi Stack Reference (DSR) Model to illustrate the technical primitives, financial functions, and compositions of DeFi protocols conceptually. As shown in Figure 1, it defines three layers, further subdivided into five sub-layers.

Settlement Layer This layer is responsible for completing financial transactions and discharging the obligations of all involved parties [22]. This involves resolution of potential conflicts and finding consensus on the current state of a system. In DeFi, this functionality is typically provided by a DLT, which implements consensus protocols and provides means for replicating the state globally across all distributed computer nodes. DLTs such as Ethereum or Solana also offer an execution environment for smart contracts, which are the core components of all DeFi protocols. DLT platforms are equipped with a native token (e.g., ETH) that represents and transfers value in transactions or in smart contract execution. Native tokens lie at the intersection of the settlement and the DLT application layer. They are cryptoassets, but are embedded in the settlement layer and are not deployed as smart contracts, unlike other non-native tokens.

DLT Application Layer It comprises applications implemented through smart contracts.

- *Cryptoassets* are DLT applications that facilitate the transfer of value across the DeFi ecosystem. They can be defined arbitrarily by anyone, simply by implementing specific "token contracts" that typically carry a name, e.g. Tether, and a symbol, e.g. USDT. A token contract can either maintain a registry of account addresses and balances (fungible token) or record token ownership (non-fungible token).
- A *DeFi Protocol* is a DLT application implemented by a set of smart contracts, utilizing cryptoassets and providing some financial service functionality. Based on the offered functionalities, we can roughly distinguish among lending protocols, derivatives protocols, and decentralized exchanges (DEXs). Functionality is realized through financial functions such as the pooling of liquidity provided by multiple users, the supply of collateral, or the swap of cryptoassets. Certain functions are specific to a particular type of protocol, while others are used in several protocols and across different categories.
- *DeFi Compositions* enable a specific type of DeFi protocol, also implemented by a set of smart contracts, that provide novel financial services by using services of other DeFi protocols. DEX Aggregators redirect users programmatically towards the DEX offering the best price for the swap of a cryptoasset pair, while Yield Aggregators implement strategies to invest user funds in other DeFi protocols and maximize their returns.

[5]Known to the public after filing for bankruptcy in July 2022 `https://reut.rs/3BAVLUj`.

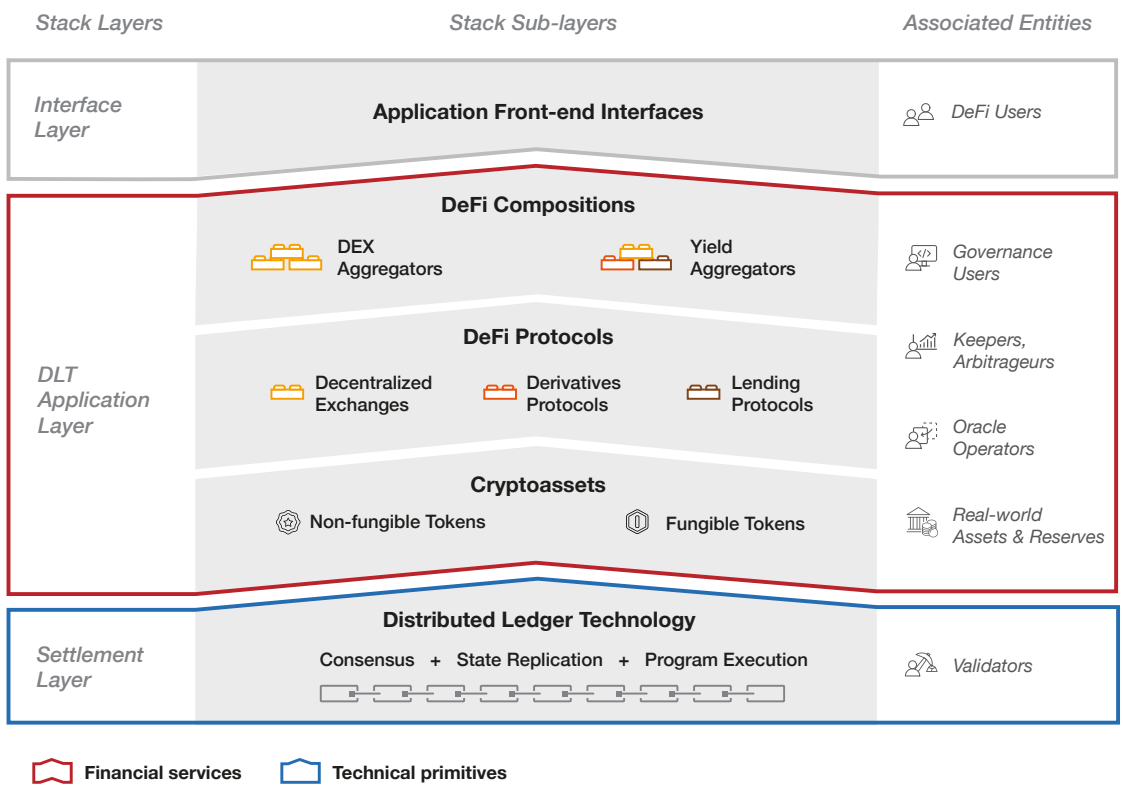

Figure 1: ***DeFi Stack Reference (DSR) Model.*** *At the foundation, the settlement layer, DLTs allow to reach an agreement on the global state of the system, replicate it across network nodes, and execute computer programs that facilitate financial transactions in return for some native token. The DLT application layer comprises arbitrary cryptoassets, DeFi protocols and DeFi compositions, offering some specific financial service, all implemented as part of smart contracts. Protocols in different categories can implement similar financial functionalities. Finally, the interface layer provides graphical front-end interfaces to DeFi users. Each layer is associated to off-chain entities: validators ensure that consensus is reached, fiat currencies are the reserves for many cryptoassets, oracles import on-chain information about real-world assets, and keepers and arbitrageurs enforce incentive mechanisms. Protocol governance is composed of DeFi users with decision-making powers. End-users interact through interfaces with DeFi protocols.*

Interface Layer DLT applications are implemented as smart contracts and provide programmatic interfaces to developers but do not offer any interactive graphical tool to the end-users. Instead, DeFi applications provide front-end interfaces that facilitate the interaction with the smart contract logic. This is typically achieved via non-blockchain applications, such as Web or mobile device applications. This layer acts mainly as a framework to provide input parameters to the DLT application layer. For the purpose of this paper, this layer is less relevant than the previous ones and thus we will not cover it in detail in the subsequent sections.

Each of these DeFi stack layers is associated with real-world entities in a broader ecosystem (see Figure 1, right-hand side column). On the lowest layer, validators are economically incentivized to process transactions and execute programs. USD, EUR, and other fiat currencies are used as a reserve by cryptoassets known as stablecoins. Financial functions like asset swapping often rely on external information: oracle operators maintain smart contracts that allow to access, within a DLT, off-chain data coming from the external world such as real-world asset prices or related exchange rates. Finally, end-users can participate as a stakeholder in the governance of a protocol or interact with a DeFi application via user interfaces.

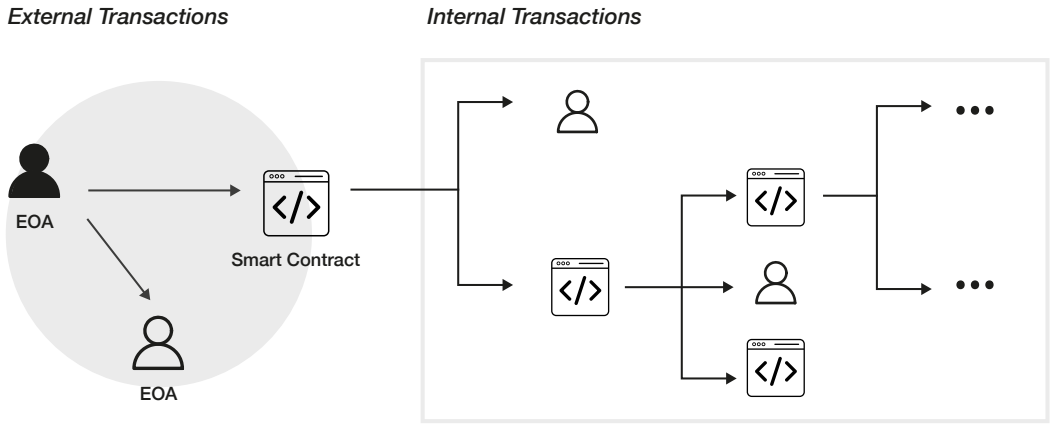

Figure 2: ***Account and Transaction Types***. *An Ethereum transaction always begins with an external transaction that can only be initiated by a user account, also known as an Externally Owned Account (EOA). It can be directed to another EOA or an account controlled by a smart contract. A smart contract can send messages (also denoted as internal transactions) to other accounts, both to EOAs and CAs. Therefore, a smart contract can produce call cascades, ie, trigger multiple contracts, which can call other contracts within the same transaction.*

3 Settlement Layer: the Technical Primitives

The entire DeFi ecosystem is built on several different DLTs. However, Ethereum represents the most relevant one in terms of invested funds and projects developed on it. Thus, in the following we will refer to it, unless specified differently.

Distributed Ledger Technology DeFi protocols are software programs running on DeFi-enabling distributed ledger technology, such as the open, permissionless Ethereum blockchain. DLTs provide transaction execution capabilities and implement consensus protocols to agree, represent and replicate system states globally without relying on a single intermediary node [43]. A key feature determining whether a DLT is suitable for DeFi is the availability of an execution environment for deploying and running smart contracts, ie software programs implementing financial functions. While the Bitcoin blockchain already provides basic mechanisms for executing custom code, its capabilities are limited [11]. Therefore, DeFi protocols typically operate on smart contract-enabled blockchains like Ethereum, and are executed by a virtual machine, like the *Ethereum Virtual Machine (EVM)*. Ethereum is still the most important blockchain for DeFi but suffers from heavy network congestion and high transaction fees [42] caused by the increasing volume of DeFi transactions. Consequently, we can observe that DeFi protocols are now deployed also on other EVM-compatible (e.g., Binance Smart Chain, Avalanche, Polygon, Arbitrum) and non-EVM-compatible (e.g., Tron, Solana, Terra) blockchains.[6] If DeFi protocols are deployed across multiple chains, one also speaks of *multichain* DeFi protocols.

State Representation: Accounts A key difference to Bitcoin is that Ethereum is an *account-based* distributed ledger. An Ethereum address identifies an account whose state is updated via state transitions through transactions. The account state stores information about the balance and the number of transactions executed. The account model thus maintains a database of account states. As Figure 2 shows, two different types of accounts exist: Externally Owned Accounts (EOAs), ie user accounts, and Code Accounts (CAs), commonly known as

[6]See `https://defillama.com/chains/Non-EVM`

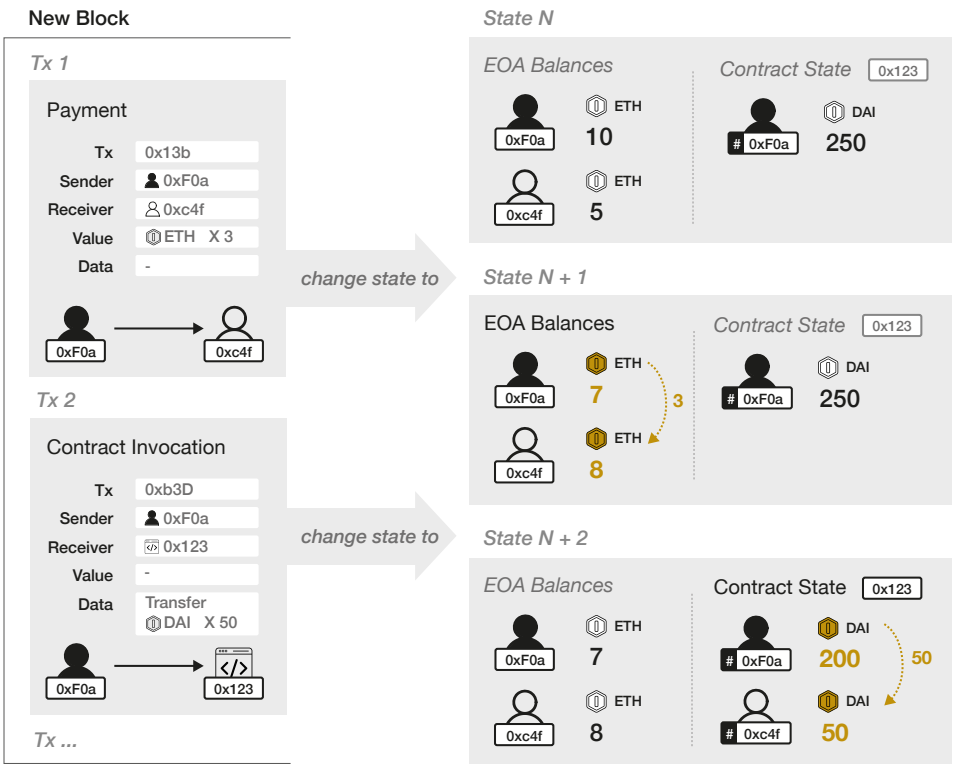

Figure 3: ***Transactions in new validated blocks and state changes***. *Transactions indicate the sender, the receiver, the Ether (ETH) sent, and the data payload. A Payment updates the state, e.g. from N to $N+1$. Ether is transferred from the sender, Alice, to the receiver, Bob. A Contract invocation changes the state to $N+2$. To transfer tokens to Bob, Alice must trigger the contract that controls them: the EVM interprets the data payload and the contract is executed. The token holders' balances, stored in a map of hashed addresses, are updated. Note that we do not account for the transaction fees in this illustrative example.*

smart contracts. EOAs can create CAs via specific transactions, also called *contract creations*. A cryptographic private key controls the former; consequently, transactions can be sent by the account owners (*external transactions*). The latter, instead, are associated with and controlled by their own code (which an EOA does not have). They do not have a private key and thus cannot broadcast transactions directly: a CA is always initially executed by an EOA. However, once executed, a CA can itself call other contracts. This can result in a cascade of contract calls, all within one individual transaction, also called *traces* or *internal transactions* [35].

State Transition: Transactions As in Bitcoin, transactions are a core element of the Ethereum blockchain, as they trigger and broadcast the intended state changes to the network. Figure 3 describes how transactions update and modify the global state of a DLT like Ethereum. By default, transactions contain, among other fields, information on the transaction Recipient, the Value, and the Data broadcast. The Recipient field is an address that indicates the receiver of the transaction.[7] Transactions with an EOA as recipient typically only contain Value, as the EOA addresses cannot interpret the managed code, and serve as payment (in Ether) among two parties. As a result, when the transaction is stored on the blockchain, the EOA account balances are updated, reflecting such state transition. Transactions executed against a smart contract contain instead a *data payload* in the Data field that triggers the CA itself. For instance, in the

[7]We note that funds lost in unintended transactions, e.g. sent to wrong addresses, cannot be recovered.

contract invocation represented on the right side of Figure 3, the sender intends to transfer 50 DAI tokens to another EOA. The external transaction is not directed to the EOA itself but to the token smart contract, and the token transfer is executed in subsequent internal transactions. The contract internally maps the EOA addresses to its internal storage, thus recording the token balance for each owner. The state change of the contract is reflected in the new internal balance of token ownership. Thus, the token balance of Ethereum accounts is handled at the smart contract level, whereas the Ether balance of Ethereum accounts is handled at the protocol level. In other words, sending Ether is an intrinsic activity of the Ethereum DLT, while sending or even owning tokens is not, and token transfers executed in internal transactions are not explicitly visible in the blockchain.

Consensus Protocols In an open, permission-less setting that allows anyone to participate, providing a robust, global state of the ledger is non-trivial. Consensus protocols solve the problem of synchronizing the account states in distributed systems such as DLTs, so that all nodes reach and maintain an agreement on it, even in the presence of malicious users [125]. In the DLT context, consensus mechanisms guarantee that new transactions, representing state changes, are appended in a unique and agreed order.

The typical assumption underlying a consensus protocol is that, in a distributed system of n independent nodes, the consensus can tolerate the failure (or malicious behavior) of a fraction of nodes $f < n/k$, where k is a parameter that varies for each consensus protocol, and the other $n - f$ nodes are not subject to failure [33]. Another approach is taken in [15], who model the underlying economic incentives that validators need to sustain an honest exchange.

Whilst many different consensus algorithms have been devised [132], the Proof-of-Work (PoW) and the Proof-of-Stake (PoS) are by far the most common ones. Bitcoin, for instance, relies on PoW to achieve consensus. Without PoW, malicious users could easily create pseudonymous accounts to undermine the authority or power of a decentralized network or to gain control over a network. This is also known as a Sybill attack. PoW prevents such attacks and provides robustness by demanding nodes to conduct computationally intensive tasks to participate in the process of adding new transactions to the blockchain (and earn rewards when elected to do so). However, this approach has downsides, such as the enormous associated energy waste [91, 39] and question marks regarding the security of payments once a cryptocurrency's block subsidy is phased out [12]. PoS is a promising alternative, where Sybil attacks are prevented by, roughly speaking, attributing to each participant in the consensus protocol a weight that is proportional to her stake as recorded in the ledger itself. At the time of writing, Ethereum already transitioned to PoS [46].

4 Cryptoassets in DeFi

Cryptoassets are used to represent and transfer value in a DLT and are, therefore, a fundamental element in the DeFi ecosystem. Current definitions for the term "cryptoasset" are non-uniform because they depend on the context (e.g., technical vs. legal) and on legal frameworks [79]. In the context of this paper, we denote as cryptoasset all digital assets that utilize cryptographic primitives and distributed ledger technology and represent some economic resource or value to someone. In a decentralized ecosystem such as DeFi they can be, amongst others, used as a means of exchange, for investment purposes, or to access a good or service.[8]

Figure 4 illustrates a (simplified) taxonomy that introduces the spectrum of cryptoassets.[9] It can be roughly divided based on the conceptual design of their underlying settlement layer: cryptoassets can either follow Bitcoin's Unspent Transaction Output (UTXO) model or Ethereum's

[8] European Banking Authority Report with advice for the European Commission on Cryptoassets [47]

[9] More detailed categorizations can be found in [79] and [84], that focus on the legal aspects, in [92] that investigates the technical aspect, and [7] that provides a more comprehensive approach including multiple aspects.

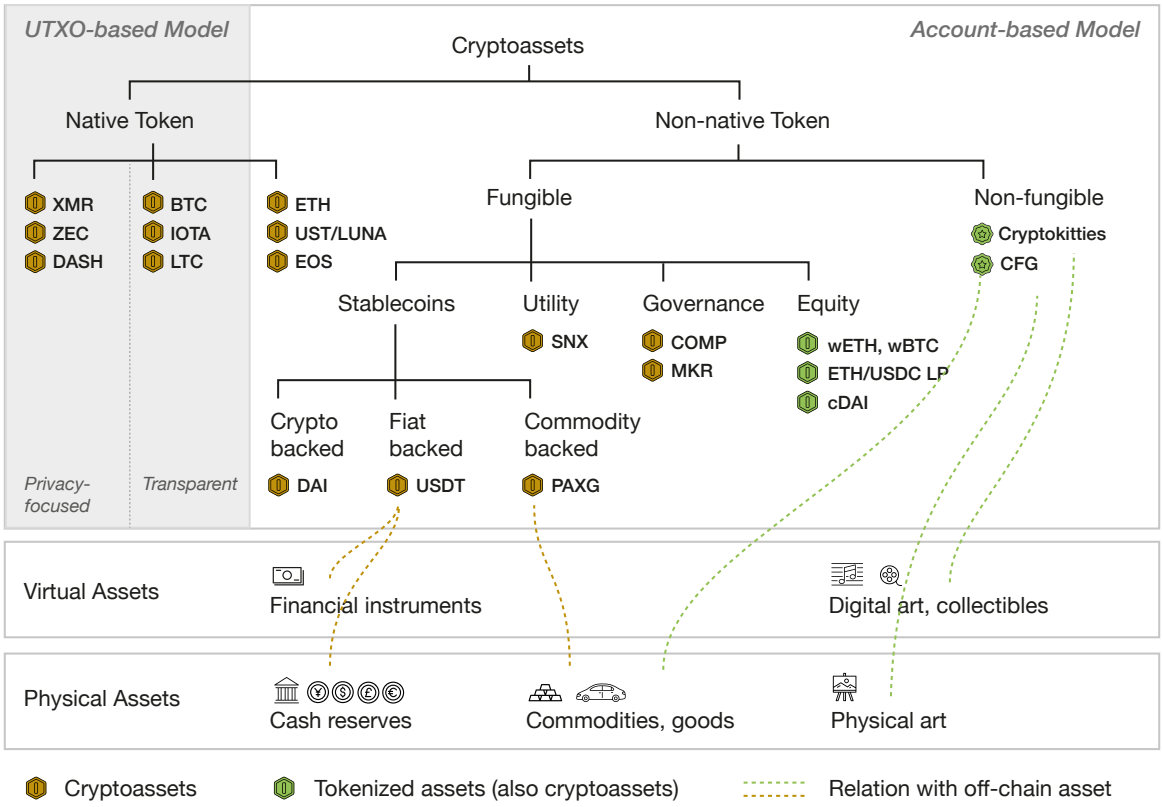

Figure 4: ***Cryptoasset Taxonomy.*** *DLTs either follow the Bitcoin-like UTXO or the Ethereum-like account model. Both support native tokens (e.g., BTC and ETH). Native tokens can further be divided into privacy-focused (e.g., XMR) or transparent ones (e.g., BTC). Account-model ledgers support the implementation of custom non-native tokens using smart contracts. These tokens can be fungible (ERC-20) or non-fungible (ERC-721). Stablecoins are fungible tokens backed by other crypto- or non-crypto assets, like fiat currencies. UTXO-based DLTs are less relevant for DeFi; thus the area is shaded in gray.*

account model. Both designs include *native tokens*, like BTC on the Bitcoin or ETH on the Ethereum ledger. Native UTXO-based tokens can be further separated into privacy-focused, such as Monero (XMR) or Zcash (ZEC), and transparent, such as Bitcoin (BTC) and other alt-coins following its design. Account-model ledgers enable the deployment of arbitrary smart contracts, thus they also allow issuing *non-native tokens* (or simply tokens). Technically, UTXO-model ledgers can create tokens too (e.g., colored coins in Bitcoin [102]). However, the programming capabilities of UTXO-based DLTs are limited and this restricts the relevant use cases of such tokens. Thus, in the following, we focus on those deployed on Ethereum-like DLTs.

Non-native tokens are used for many purposes, from the definition of custom currencies, over the representation of ownership or membership claims, to representing access credentials for software games. Since the spectrum of token use can hardly be limited, categorizing based on utility is difficult. However, it is possible to clearly distinguish tokens based on their technical design as they follow a specific standard, which defines a predefined minimum set of functions to be implemented by the smart contract controlling a token.[10] The two primary token standards are ERC-20 and ERC-721, which respectively define a common interface to create *fungible tokens* and *non-fungible tokens* (NFTs).

Non-fungible tokens (NFTs) are typically used to represent and uniquely identify some specific virtual asset, such as digital art or a collectible [88]. More recently, NFTs are also issued for

[10] All non-native token accounting activity is handled at the smart contract level; on the other side, balances and transfers of native tokens are handled at the settlement level.

guaranteeing ownership of physical items such as sports collectibles, antiques, or even consumer goods. Most DeFi applications do not yet rely on NFTs; however, recent developments indicate that NFTs could, for instance, be used for loan collateralization or controlling fractional ownership.[11] Protocols like Centrifuge with its token CFG promise to bridge even real-world physical assets to DeFi, by representing them on the blockchain (on-chain) as NFTs.[12]

Fungible tokens are intrinsically indistinguishable. As mentioned above, they can be utilized for many purposes. In the context of DeFi, an example of a *utility token* is SNX, which is used as collateral in the Synthetix protocol and enables access to specific smart contract functions. ETH/USDC LP is an example of an *equity token*, representing claims on shares of underlying assets, in this specific case being a claim on the amount of ETH and USDC deposited as liquidity provision (LP) in the Uniswap DEX.[13] It is used in the Uniswap protocol as a deposit certificate for the ETH and USDC trading pair. Another important use case for fungible tokens in DeFi is that of *governance tokens*, which allow users to become stakeholders with voting rights and decision-making power in the governance structure of a DeFi protocol [113]. MKR and COMP are governance token examples of the protocols *MakerDAO* and Compound. Typically, governance tokens are distributed to protocol users and grant rights in fractional shares proportional to the held amounts. However, recent research has shown that DeFi governance is often de-facto centralized and usually composed of protocol insiders and developers [17, 66].

Another relevant type of cryptoasset, defined by its mechanism design rather than by the technical aspects, is that of stablecoins. Their goal is to stabilize the price and volatility of a token [87, 73] by pegging their value to some external reference asset. Stablecoins can be implemented as ERC-20 tokens, e.g., DAI, USD Coin (USDC), Tether (USDT), or as a native asset like UST in the Terra chain. The first and most important design choice of a stablecoin is the price target or peg: it can be the USD price (DAI, USDT, USDC, UST) or commodities such as metals (PAX Gold, or PAXG). The second choice regards the stabilization mechanism: in many cases, stabilization is reached using the targeted asset or other liquid assets as collateral. USDC, for instance, is backed almost entirely by cash, bank deposits, and Treasury bills. Tether (USDT), on the other hand, is also backed with commercial paper and corporate bonds [65]. USDC and USDT are *centralized* stablecoins: their issuance and redemption on-chain corresponds to fiat transactions, executed off-chain, between the token governance and the investors.[14] Thus, their issuance is not automated and relies on commercial banks. *Decentralized* stablecoins like DAI are instead backed with other cryptoassets (ETH, USDC, wBTC) and are fully automated and non-custodial. Finally, some stablecoins rely on algorithmic-based approaches, whereby supply is adjusted programmatically as a response to specific market conditions (e.g., Ampleforth), or dual coin systems reach price stabilization as in the case of Terra tokens UST and LUNA. In this mechanism, the stablecoin price (UST) is related by design to that of another token that absorbs all volatility, and arbitrage mechanisms incentivize users to hold the volatile one [104]. The collapse of Terra, however, showed that stability pledges of algorithmic stablecoins are not guaranteed and that they are susceptible to "stablecoin runs" [74].

In general, asset tokenization [106] is an essential feature in DeFi. By implementing a dedicated token contract, one can represent any other on- or off-chain asset on a given DLT platform. On Ethereum, for example, one can issue *wrapped tokens*, ie, ERC-20 compatible versions of other cryptoassets. The wrapped BTC (wBTC) token is a prominent example and allows users to use Bitcoin in the Ethereum DLT [27]. It is 1:1 backed with Bitcoin.[15] Since wrapped tokens often derive their value from some other (underlying) asset, one could argue that existing assets that have been tokenized are generally a form of derivative [118].

[11] See respectively `https://bit.ly/3V1qCQQ` and `https://fractional.art/`

[12] `https://centrifuge.io/`

[13] This token is issued upon interaction with the V2 version. At the time of writing, Uniswap also implemented the V3 version, in which the claimant receives an NFT representing fractional ownership of the protocol liquidity.

[14] See `https://tether.to/en/how-it-works/`

[15] `https://wbtc.network/`

5 DeFi Protocols

After introducing cryptoassets as a core stack layer component in the DeFi ecosystem, we now focus on the DeFi protocols, which provide higher-level financial services built on top of them, such as borrowing, lending, or trading. Since the term is not yet clearly defined, as a starting point, we define it for the purpose of this paper as follows:

Definition 2 *A **DeFi protocol** provides one or more financial services to economic agents. Financial services are implemented as program functions by one or more smart contracts.*

Typically, a DeFi protocol and its underlying smart contracts are developed by a team of developers as part of a specific project. While it is not straightforward to delineate precise boundaries between protocols, for this paper, we identify the following main categories that describe well most of the existing relevant DeFi protocols:

- **Decentralized exchanges** (DEXs) facilitate the exchange of cryptoassets.
- **Lending protocols** allow users to lend and borrow cryptoassets.
- **Derivatives protocols** are trading platforms where investors can issue and trade synthetic positions that track the value of underlying crypto- or real-world assets.

Aggregation services like yield aggregators, which implement automated portfolio optimization strategies and act as decentralized investment funds, are DeFi applications that provide novel financial services by exploiting smart contracts composability. We thus discuss them in Section 6.

Next, we describe, for each category, the main design mechanisms, the most important financial services they offer, and the economic agents involved. We illustrate the functionality of one representative DeFi protocol in each category and the main interactions with the economic agents involved.[16] We also compare these services to those offered by traditional finance institutions. In this section, we focus on protocols deployed on Ethereum.

5.1 Decentralized Exchanges

Decentralized exchanges (DEXs) are DeFi protocols that facilitate the programmatic exchange of cryptoassets. Their design can follow two main models: order book DEXs such as *0x* [120] and *EtherDelta* [45], which exploit the same model deployed in centralized trading platforms, and DEXs with Automated Market Makers (AMMs) [128]. Most of the current research focuses on the latter, aiming at better investigating their innovative design, and for this reason we focus our attention on them. Different from traditional (and decentralized) order book-based exchanges, in which price discovery depends on the matching mechanism of the buy and sell orders placed by the traders, the AMM-based DEXs [20, 80, 82] exploit a peer-to-pool mechanism: for each supported trading pair, a protocol-specific smart contract *pools* the cryptoasset reserves supplied by many individual liquidity providers, acting de facto as an Automated Market Maker (AMM), and incoming trades are executed against these pools.

Financial Services Figure 5 describes the services offered by DEXs and the economic agents they interact with, using the protocol *Uniswap V2* [3] as a reference. The core financial service of DEXs is to facilitate the *swap* of tokens. A swap is a simple token exchange that a *Trader* executes against a liquidity pool smart contract that holds reserves x and y of a token pair (e.g., Token_x and Token_y). For most AMMs, the swap pricing mechanism depends on invariant

[16] The interactions illustrated in Figures 5 to 7 and 10 are constructed after conducting manual transactions with the mentioned protocols, to fact-check and verify the correspondence with the reported documentation.

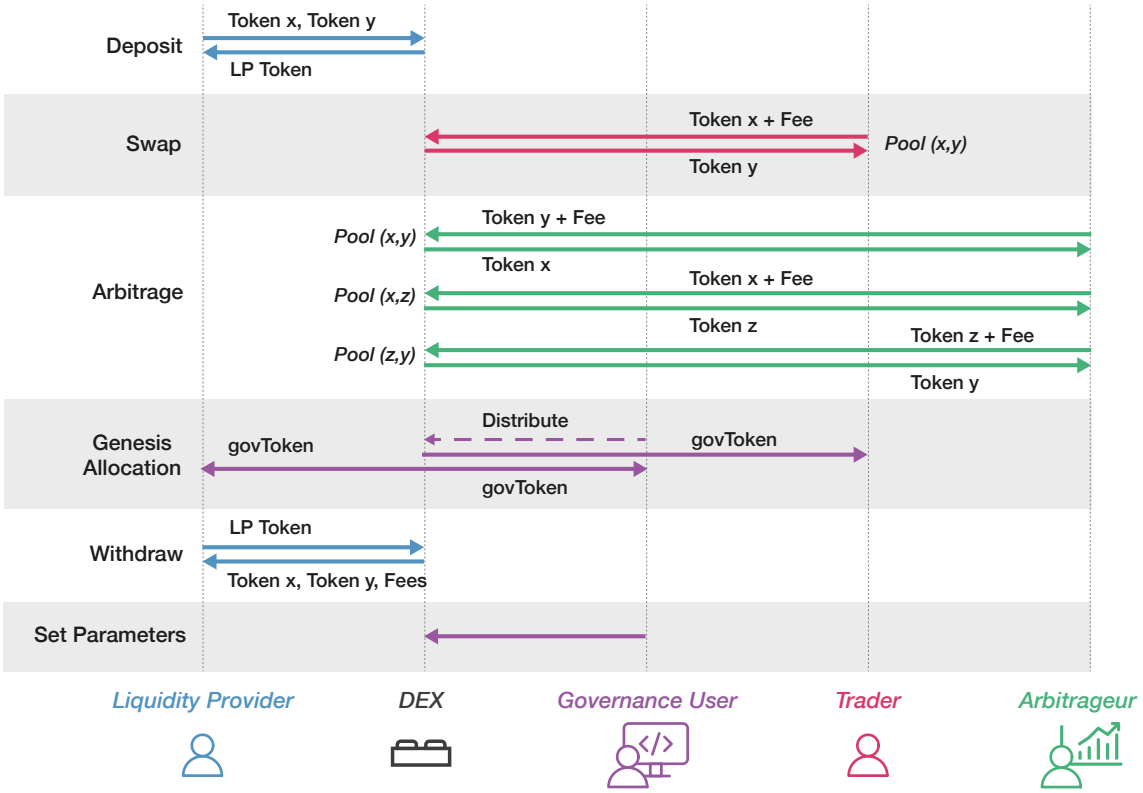

Figure 5: ***AMM-based decentralized exchange (DEX)***. *Traders are DeFi users who exchange (swap) tokens, while Liquidity providers (LPs) deposit and withdraw liquidity in or from pools specific to each trading pair. Arbitrageurs rebalance pool compositions when imbalances emerge. Users holding governance tokens have voting rights and decision-making power and receive fees from users swapping tokens.*

properties such as the *conservation function* that binds the pooled reserves of the two assets [5]. In the simplest case of a constant product function (CPF), the reserves are constrained by the equation $f(x, y) = x \cdot y = k$. *UniSwap*'s V1 and V2 versions implement this bonding curve.[17]

The spot exchange rate is the token reserve ratio. When a swap is executed, a trader deposits an amount Δx to the trading pair liquidity pool, and withdraws Δy such that the condition $(x + \Delta x) \cdot (y - \Delta y) = k$ is met [6]. Thus, large enough swaps can cause slippage, ie, a difference between the spot and the realized price. Incentive mechanisms ensure price convergence: *Arbitrageurs* rebalance pools for profit by conducting trades opposite to the price slippage. Figure 5 illustrates the execution of a cyclic arbitrage strategy [119] across pools of the same DEX. An alternative strategy is to conduct arbitrage on the same trading pair across different DEXs [37].

In order to facilitate token swaps, *liquidity pooling* plays an essential role. DEXs exploit smart contract-based financial functions that enable the deposit and withdrawal of token pairs in or from the liquidity pool smart contracts. Any owner of a pair of tokens can become a *Liquidity provider* (LP) by locking them in a liquidity pool [30]. In turn, *LP tokens* are minted and supplied to the LP, proportionally to the amount of cryptoassets provided. Thus, LP tokens represent pool shares and grant a claim to withdraw a fraction of the underlying funds when they are burnt. In this sense, they are an example of asset tokenization, as they represent fractional ownership of the underlying pool. Deposits typically respect the ratio established by the market

[17] See [2, 3]. The latest version, V3, is based on a similar mechanism but introduces a more complex function [4]. Other common types of conservative functions are the constant sum [75] and the geometric mean [48, 49].

price[18] to prevent the rise of arbitrage opportunities: a pure liquidity provision action does not modify the implied exchange rate but rather affects the parameter k [30].

Incentive mechanisms foster liquidity provision. As LPs take on price risk, they are rewarded with fees: for each swap, a fee is charged to the trader, and it is further divided between LP shareholders.[19] Part of the fees can be retained in the protocol[20] and managed by the governance, ie, users who hold UNI, the protocol's governance token. Governance tokens' ownership grants voting rights: owners can vote on design choices and propose strategic decisions such as modifying protocol parameters (slippage control, fees) or deciding how to use the protocol treasury. The UNI governance tokens were minted at the "Genesis"[21] and distributed, according to a teams' decision, for a limited time to the team itself and to all protocol users as a reward for participation. The practice of including governance tokens as a further incentive for protocol users, and especially for LPs, is called liquidity mining [50]. For the period where liquidity mining was active, governance tokens would appear in all user interactions with the protocol in Figure 5; we thus show their distribution as a separate interaction to increase readability and to underline that liquidity mining was active in *Uniswap* only for a short time window. Other DEXs, such as *Sushiswap* and *Curve*, exploit more systematically liquidity mining programs.

Other Examples Other DEXs play a relevant role in DeFi and thus deserve special consideration. *SushiSwap* [114], for instance, is a popular protocol created by forking *UniSwap*; their mechanism design is similar. *Curve* [96] focuses on pools of cryptoassets with the same underlying asset (e.g., USD-pegged stablecoins or Bitcoin-based cryptoassets) and implements a constant function that allows for concentration liquidity in smaller price ranges. *Balancer* [86] and *Bancor* [63] are two other relevant AMMs in terms of TVL. The first allows constructing pools of multiple cryptoassets, while the latter supports single-asset liquidity provision.

5.2 Lending Protocols

Protocols for loanable funds (PLFs) [19], also referred to as lending protocols, automate the borrowing and lending of cryptoassets. In doing so, they facilitate the efficient allocation of capital within the DeFi ecosystem [9]. PLFs operate in a peer-to-pool fashion: borrowers interact with smart contracts that *pool the liquidity*, ie, resources supplied by cryptoasset lenders. An essential difference to loans issued by traditional financial institutions is that interest rates are set automatically [129], mostly depending on market conditions such as the demand for loans or the pool size, as well as on parameters decided at the governance level. Interest rates can be influenced by systematic and protocol specific risk factors [64].

Financial Services Figure 6 shows how the economic agents interact with financial services offered by lending protocols such as *Compound* [81]. The core service is token *lending and borrowing*. *Lenders* deposit funds, and in return, they receive tokenized assets that allow them to redeem deposits later in time, plus an additional interest rate. For example, the PLF *Compound* generates wrapped tokens (cTokens) whose exchange rate against the underlying asset constantly grows in time [103]. Thus, when funds are redeemed, their value has increased. On the contrary, *Borrowers* pay interest on their open positions before closing them. *Compound* interest rates follow a threshold-based model, ie they rise sharply after a specific borrowing utilization ratio against the deposited funds, while other PLFs follow linear and non-linear models [60].

The *collateralization* of debt positions is a core financial function PLF contracts build upon. Typically, borrowing is allowed only after collateral provision as a protection against the coun-

[18] However, some AMM-based DEXs like Bancor support single-sided liquidity provision; Balancer allows to decompose large LP actions into swaps and balanced LP actions [128].

[19] See `https://docs.uniswap.org/contracts/v2/concepts/advanced-topics/fees`

[20] At the time of writing, *Uniswap* doe not retain fees, unlike other DEXs such as *Sushiswap* [55].

[21] See `https://uniswap.org/blog/uni`

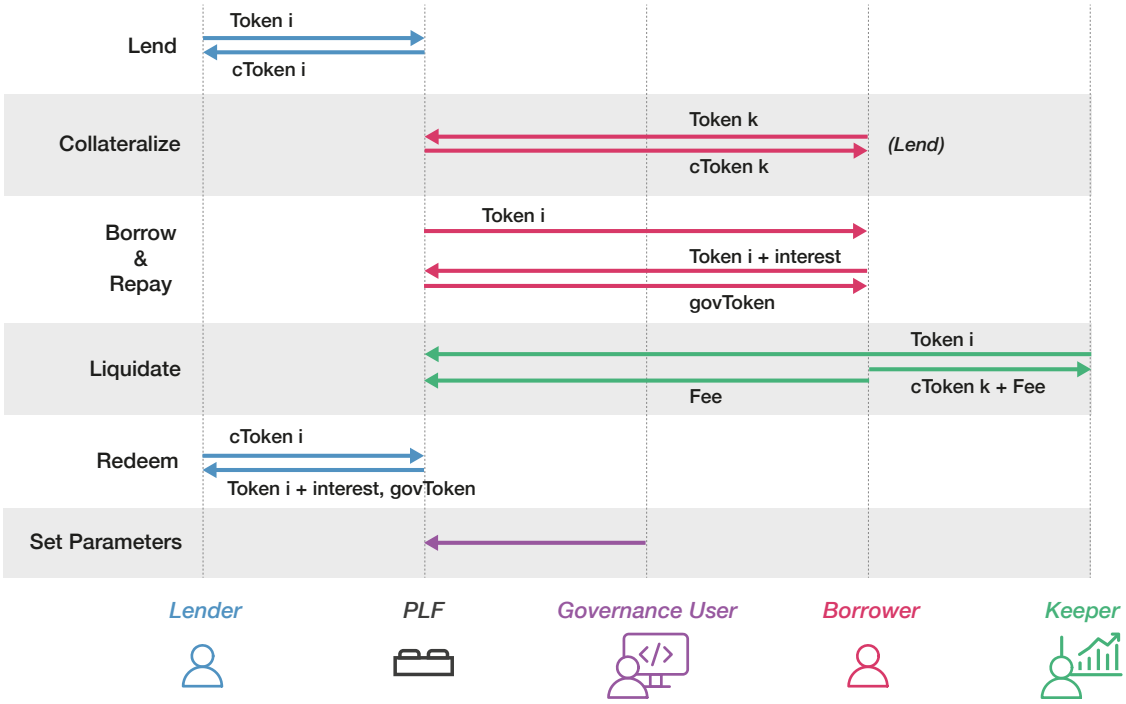

Figure 6: ***Lending protocol***. *Borrowers take out loans on funds supplied by Lenders, and their default risk is hedged by overcollateralizing their positions. Keepers close insufficiently collateralized positions for a fee. Governance members earn fees from protocol usage.*

terparty risk of default.[22] PLFs often require such positions to be overcollateralized due to cryptoassets volatility and to counterparty anonymity [9]. In *Compound*, collateral is provided by interacting with the same contract functions that serve to supply liquidity;[23] thus, borrowers earn interest on collateral. DeFi users can then borrow other cryptoassets. The interests paid on borrows create the reserves to pay the lenders' interests.

Price fluctuations can lead to insufficiently collateralized positions: if the borrower does not provide additional capital, the loan may be liquidated [94]. *Keepers* are EOAs that monitor the market, searching for insufficiently collateralized loans (liquidations are implemented as contract calls, thus, they must be initiated by EOAs). In *Compound*, by design keepers can repay only part of the borrowed position, and receive in return a fraction of the borrower's collateral at a discount with respect to the market price [68]. At the new market prices, either the remaining borrower's collateral is sufficient to back the fraction of loaned cryptoassets that were not liquidated,[24] or it will be subject to subsequent liquidations. Part of the fees can be retained within the protocol.[25] The PLF *Aave* exploits a similar mechanism to *Compound*, but it grants higher discounts to liquidators. In other protocols, such as *MakerDAO*, keepers can auction the collateral, repay the loan, and receive a fee for enforcing the liquidation [97]. In *Compound*, protocol usage is directly rewarded with governance tokens, as part of liquidity mining programs to incentivize usage. Governance members can vote proposals on changes regarding, e.g., the tokens accepted, the collateralization thresholds, parameters establishing the interest rates, and other design aspects.

[22] Flash loans are instead an uncollateralized lending mechanism enabled by DeFi that eliminates default risk: loans are either atomically executed and repaid within one individual transaction or reverted [99].

[23] See `https://medium.com/compound-finance/borrowing-assets-from-compound-quick-start-guide-f5e69af4b8f4`

[24] See `https://zengo.com/understanding-compounds-liquidation/`

[25] See `https://docs.compound.finance/v2/comptroller`

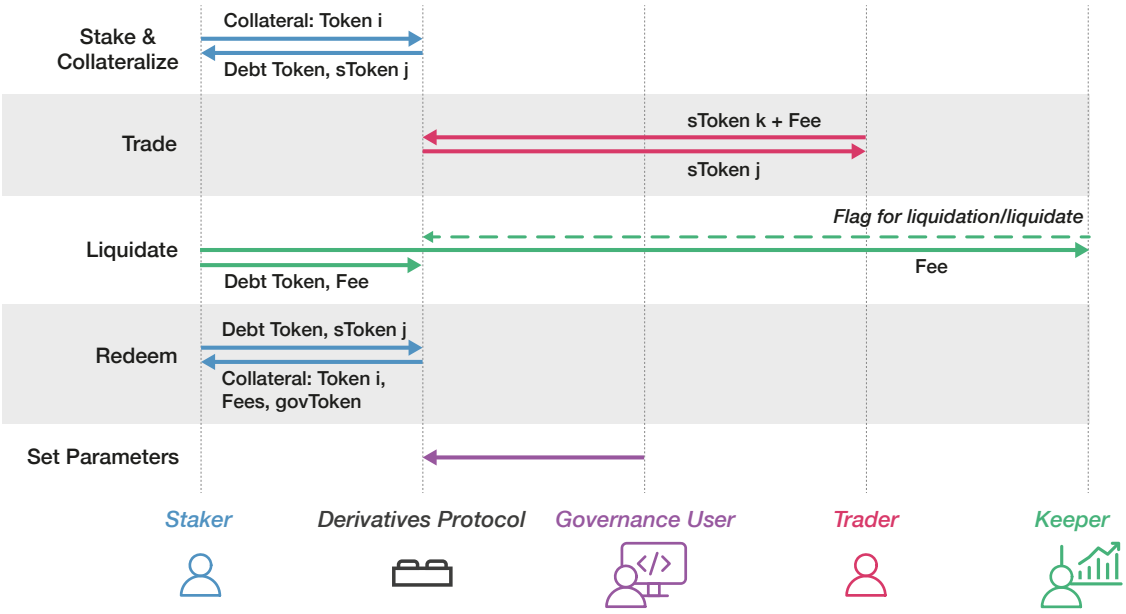

Figure 7: ***Derivatives protocols***. *Stakers supply capital in a pooling contract for a reward, Traders can swap derivative products like in DEXs. Similarly to PLFs, Liquidators auction insufficiently collateralized positions.*

Other Examples *Aave* [1] is among the largest PLFs by total value locked. It provides similar financial services to *Compound*, and users can choose between stable and variable interest rates. *MakerDAO* [85] is another lending protocol that allows locking capital to mint DAI. Other relevant protocols categorized as PLFs are *Alpha Homora* [38] and *Liquity* [78].

5.3 Derivatives Protocols

We now consider the protocols that issue and facilitate the trading of financial derivative contracts in a decentralized context. While DEXs and PLFs have been investigated deeply, the academic literature on derivatives protocols is scarcer. DeFi derivatives are cryptoassets that track the price of an underlying asset that can be another cryptoasset, a traditional financial asset, a commodity, or priced real-world events [76]. The spectrum of derivatives protocols ranges from call and put options over futures, forward contracts, and perpetual swaps [111]. Synthetic assets enable exposure to an asset without actual ownership. To trace the underlying assets' price, these DeFi protocols exploit *Oracles*, ie, smart contracts that act as a bridge service between a DLT and the external world, allowing to retrieve real-world, off-chain data [107]. While centralized finance investors rely on intermediaries that accept and settle orders, derivatives DeFi protocols substitute them with smart contracts that issue the financial instruments at conditions determined automatedly, upon the provision of collateral as a protection against risks.

Financial Services Figure 7 illustrates the interactions between a derivatives protocol and the economic agents involved, using as a reference the protocol *Synthetix* [115]. This platform focuses primarily on synthetic perpetual contracts, or *synths*, which allow users to bet on future prices without an expiration date and to replicate the payoff of an underlying asset without owning it. It supports real-world assets, such as fiat currencies and commodities, as well as cryptoassets and indexes that track the general DeFi market dynamics.

As for PLFs, *overcollateralization* is a key element of the protocol design. *Stakers* must

provide ETH or SNX, the token native to the protocol, to issue synths (sTokens) representing the derivative contract, and a "debt" token that tracks the amount of generated synths is issued too.[26] Both are tokenized assets. To unlock the staked collateral, users burn the synths as well as the debt token. The debt issuance relies on a *pooling* mechanism: when investors issue synths, debt tokens are generated as a fraction of the overall debt in the system. The latter fluctuates to reflect the price changes of the underlying assets. Thus, when the price of an asset changes, the individual staker's debt is affected independently of the position held for this specific asset. Stakers act thus as a pooled counterparty to all Synth exchanges [115].

Once synths are minted, *Traders* can *swap* them or bet on their future prices on dedicated platforms that integrate and complement the contract issuing process. While the trading activity is subject to the payment of a fee, the staking activity is rewarded in two main ways. First, *Stakers* obtain a reward when they withdraw their collateral through a liquidity mining program: Synthetix adopts an inflationary monetary policy, and stakers can claim the newly minted SNX when they burn synth tokens to redeem their collateral. Second, Stakers earn a fraction of the fees paid by the Traders, proportional to the staked capital. Fees are partly retained in the protocol treasury and are used to pay a salary to some governance members.[27]

Derivatives protocols rely as well on other users to enforce incentive mechanisms. Arbitrage further ensures price convergence: if synth prices diverge from the underlying assets, e.g., if a synthetic asset is undervalued, arbitrageurs can buy it cheaply elsewhere and exploit it within the protocol ecosystem, where market values are not considered. Additionally, insufficiently collateralized positions are liquidated by *Keepers* that receive a fee for identifying them and to initiate liquidations at a penalty for the staker. The penalty is then redistributed to the other stakers, while the remaining collateral is returned to the liquidated account.[28]

Other Examples Other relevant derivatives protocols are *dYdX* [67] and *Nexus* [69]. The former, similarly to *Synthetix*, offers perpetual contracts, and in addition, it allows to conduct margin trades. The latter, instead, focuses on providing insurance instruments to hedge risk in investment strategies. *Barnbridge* [18] offers tools to tokenize and hence hedge risk, while *Hegic* [122] offers many different derivative contract options.

5.4 The DeFi Peer-to-Pool Model: A Generalization Framework

After describing the main DeFi protocol categories and their mechanism designs, we now abstract the DeFi protocols and the financial services they provide in a generalized framework that applies to most[29] of them with minor specializations.

First, protocols typically provide services based on the ability to *pool* cryptoassets. Figure 8 illustrates this concept, which is defined as the peer-to-pool model [130, 128]. Smart contracts are used to custody or escrow the cryptoassets of capital providers that lock up their funds, e.g. to provide liquidity in DEXs or as collateral in PLFs. Asset pooling represents the primary way to raise liquidity in the DeFi ecosystem, and it allows financial transactions not to depend on matching mechanisms or interactions with a peer counterparty. Rather, DeFi services are automated and the outcomes are deterministic, as the financial functions follow the logic described in the smart contract itself.

Service customers that actively demand liquidity, by accessing DeFi protocols services such as the borrow or swap of cryptoassets, pay fees or interest rates upon usage. Capital providers passively earn revenues and take part into liquidity mining programs, as a reward for taking risks such as price risk for LPs, and since they improve the services provided by the protocols

[26] See `https://blog.synthetix.io/basics-of-staking-snx-2022/`

[27] See `https://docs.synthetix.io/governance/` and `https://kwenta.io/dashboard/markets/`

[28] See `https://blog.synthetix.io/new-liquidation-mechanism/`

[29] With some exceptions, such as order book-based DeFi protocols.

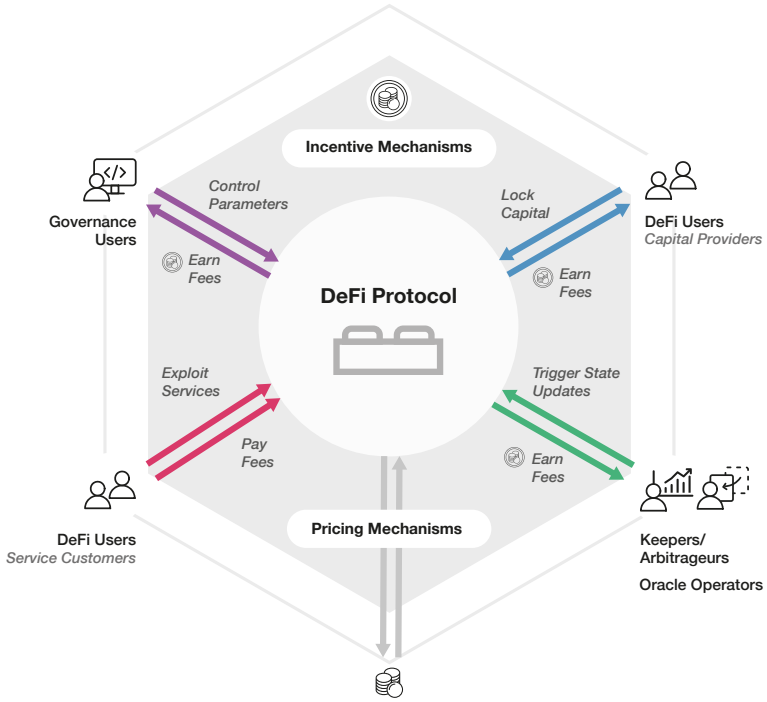

Figure 8: ***DeFi Peer-to-Pool Model.*** *Generalization of the interactions between economic actors and the DeFi protocols. The DeFi users that exploit the protocols by demanding liquidity pay a fee for accessing their services, while those that provide liquidity passively interact with them and earn an income for supplying liquidity. All other economic agents (Governance users, Keepers, Arbitrageurs) are moved by economic incentives to participate in the DeFi ecosystem.*

by supplying liquidity. Their claims over the locked cryptoassets are typically handled with tokenized assets that prove ownership and enable owners to withdraw the underlying asset.

Beyond the fees paid to capital providers, protocols incorporate other incentive mechanisms. Keepers initiate for a fee transactions that cannot be triggered automatically by smart contracts, and arbitrageurs conduct profitable trading activity, ensuring price convergence. Oracles are a relevant component of DeFi as well. Their operators ingest data (state updates) and collect fees for the service provided, enabling the interaction with off-chain data. Protocol token ownership grants the governance members decision-making power and voting rights.

Finally, also pricing mechanisms are similar across protocols. Token supplies are handled by burning and minting them to adjust scarcity. Stablecoins prices are stabilized using collateral as a reserve or via alternative algorithmic methods such as dual coins. This mechanism allows matching the price of any financial asset, also of derivatives contracts [104]. DEXs exploit bonding curves and conservation pricing functions to price assets relative to one another, and Oracles are exploited to incorporate external sources of information into the protocol.

6 DeFi Compositions

Up to now, we have considered DeFi protocols as distinct, independent entities. However, DeFi protocols can also be arranged through so-called "DeFi compositions" to offer new financial services that exploit financial functions provided by other DeFi protocols [44, 116]. Since composability has become a central aspect of current DeFi developments [118], we now focus on protocol interactions at the smart contract level.

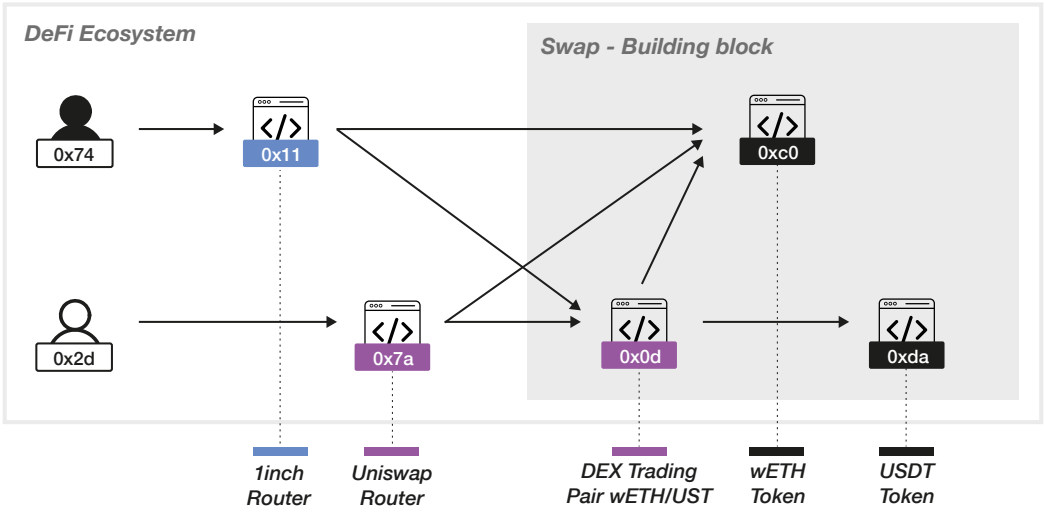

Figure 9: ***DeFi Composition Example***. *Illustration of two distinct transactions at the smart contract level. The colored rectangles indicate protocol-specific smart contracts, and the colors are used to distinguish those associated with different DeFi protocols (blue for 1inch and pink for UniSwap). To swap tokens, a user can interact with UniSwap's router or 1inch's router: both produce the same interaction with the UniSwap DEX Trading Pair contract. The top transaction is an example of DeFi composition.*

6.1 Conceptualization

To illustrate the concept of a DeFi composition, we refer to Figure 9. It shows the execution of two transactions at the smart contract level. Both trigger the *same* financial service, ie, a swap of two tokens (wETH and USDT) executed by the *UniSwap* contract "DEX Trading Pair". The one on top is initiated by an EOA triggering the "Router" smart contract of the *1inch* protocol, while the one on the bottom is directed to *UniSwap*'s "Router" contract. The purpose of the *1inch* contract is to compare prices across several DEXs and to route the user to the one offering the best price for the swap. In this illustrative example, the target protocol with the best prices is *UniSwap*. Thus, the transaction directed to *1inch* is an example of a DeFi composition: the *1inch* protocol provides a novel financial service, ie, it compares prices and liquidity *across* DEXs, and interacts with smart contracts associated with other DeFi protocols.

In the above example, a smart contract triggers multiple contracts that subsequently call other contracts. This call cascade happens *within the same transaction* executed by the end user, who controls one or more Externally Owned Accounts (EOA). Given this conceptualization, and following [72], we define the notion of a "DeFi Composition" as follows:

Definition 3 *A **DeFi composition** provides novel financial services by utilizing a combination of multiple DeFi protocol-specific smart contracts within a single transaction.*

6.2 Aggregators

At the time of writing, the most relevant implementation of DeFi compositions regards the category of Aggregators. The example described above introduces *1inch*, a DeFi application that analyzes prices on different DEXs and automatically routes the users to the one offering the best price. *1inch* can be thought of as a *demand-side* Aggregator, that is, it redirects users programmatically towards the DEX offering the best price for a cryptoasset. Even more important are the *supply-side* Aggregators, also known as Yield Aggregators, ie services that implement strategies to maximize the users return across multiple DeFi protocols.

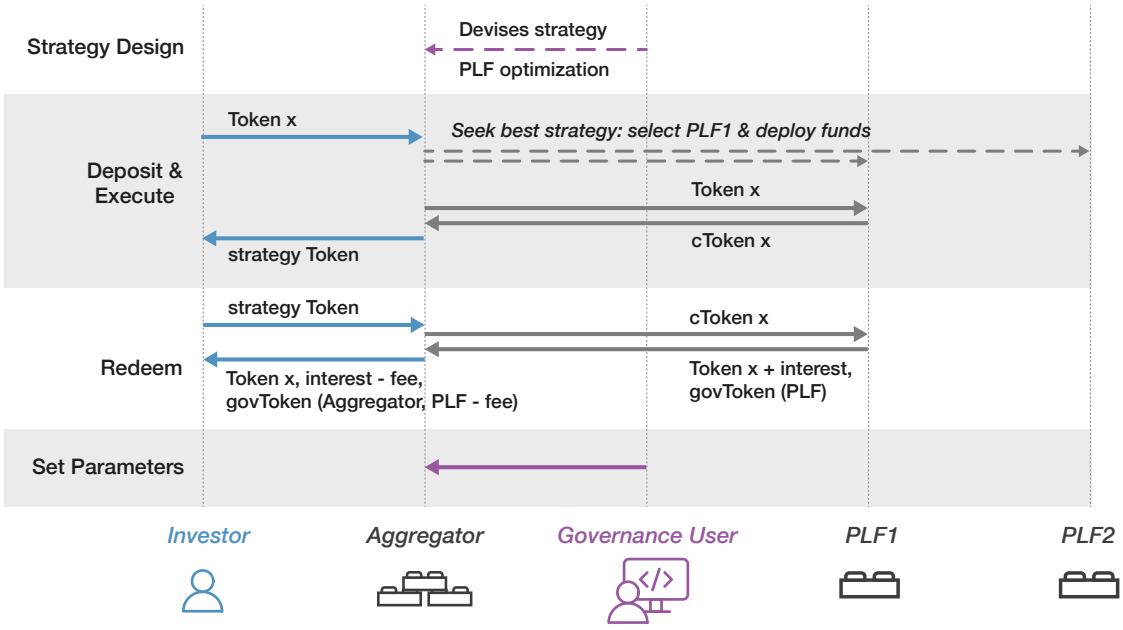

Figure 10: ***Yield Aggregators***. *The Governance proposes yield farming investment strategies to Investors who lock their capital to a "Vault" smart contract. The Aggregator in turn interacts with other DeFi protocols.*

Yield Aggregators [127] aim to maximize the value of a cryptoasset portfolio by comparing the returns of diversified financial services across multiple DeFi protocols. The concept of moving assets across protocols following optimized investment strategies is called yield farming [95]. The optimization strategies and the underlying assets differ across protocols, but their primary mechanism is similar: users lock capital in a contract (also called Vault) that allocates it programmatically to a set of other DeFi financial instruments, according to user preferences, such as risk profiles, and governance parameters [107]. Yield aggregators work similarly to traditional investment funds, the key difference being that the peer-to-pool mechanism does not require brokers or custodians.

Financial Services Figure 10 describes the general mechanisms of the yield aggregators and the economic actors involved. It is based on the protocol *Idle Finance* [52]. Compared to DEXs and PLFs, the *Governance* has a more prominent role, as the core financial service provided by yield aggregators is the design and deployment of *optimization strategies*. These are proposed by the protocol development team and/or voted by the governance members, and the yield aggregator protocol acts as an automated fund manager. However, in some cases, strategies are semi-automatic, and fund managers play an active role [107].

Once a strategy is devised, a Vault contract is created. In *Idle*'s Best Yield strategy,[30] the Vault collects single cryptoassets supplied by individual *Investors*, which in turn receive strategy tokens, ie tokenized assets that represent fractional ownership of the total invested capital. These are minted upon capital provision and can be burnt to redeem it. The strategy execution thus depends critically on the *liquidity pooling* phase. More generally, the pool compositions may differ across strategies, e.g., pools can collect tokens such as wrapped tokens and tokenized assets, but also basket of tokens as in *Rari Capital* [36].

Once funds are collected, Yield aggregators deploy the funds in strategies that entail investing them in other yield-bearing DeFi protocols. In the example described above, the yield farming strategy involves the PLF *Compound*. Other Aggregators exploit also DEXs and their liquidity

[30] See `https://docs.idle.finance/products/best-yield`

mining programs. For instance, *Harvest Finance* implements DEX-based strategies where funds are deposited in liquidity pools and the protocol collects and redistributes liquidity mining rewards.[31] Thus, when investors redeem their funds, they profit in multiple ways: they receive governance tokens from the Yield Aggregator itself, as well as revenues from investment in other protocols both in the form of trading fees (DEXs) or interest rates (PLFs) and of governance tokens of the targeted protocols. Yield Aggregators retain a performance fee on the revenues.

Other Examples Besides *Idle Finance*, Aggregators such as *Pickle Finance* [53] base their strategies on investing in LP tokens associated with liquidity pools with the highest returns on investment. *Harvest Finance* [51] offers the possibility to choose between both strategies. Others, like *Yearn Finance* [54], offer several products that entail more complex strategies that combine multiple protocols and exploit leveraged positions or explicitly base their yield strategies on stablecoins such as *Fei* [105] or wBTC such as *Badger* [16].

6.3 Investigating DeFi Compositions

The example illustrated in Figure 9 shows a simple nested structure in which *1inch* uses the "swap" financial functionality of *UniSwap* to interact with the DEX trading pairs wETH and USDT, and Figure 10 describes how Aggregators exploit financial services provided by other protocols. However, previous work [71] has shown that the compositions can be deeply nested and involve several DeFi protocols at multiple levels of depth. The term "financial lego" is often used to illustrate that multiple protocol-specific smart contracts can be assembled or composed, offering some novel financial service. As discussed in Section 1, there is a clear need to investigate and better understand such compositions. To do so, and following [72], we identified two possible directions that we describe below.

Building Block Extraction Disentangling the building blocks of DeFi compositions is one possible investigation approach. In this context, a building block is a general pattern that appears in multiple transactions but consistently implements the same financial functionality. Consider, for instance, again Figure 9: the "Swap" building block always has the same structure, independently of the tokens involved in the swap. Noteworthy, building blocks can also contain other building blocks in a nested structure. In [71], we proposed an algorithm to identify such building blocks and measure their occurrence in Ethereum transactions. Building block extraction can contribute to a better understanding of a new family of financial products and could play an essential role in assessing systemic risks if DeFi is increasingly adopted.

The DeFi Contract and Protocol Networks Another possible investigation approach is to analyze the interdependencies between smart contracts that can be attributed to specific DeFi protocols. One can extract these interdependencies from transactions involving smart contracts of DeFi protocols and construct a network abstraction in which a node represents a smart contract and edges the aggregation of all transactions involving a specific source and target contract. Further, one can merge all the contracts specific to the same protocol into a single node and investigate the network interactions at the protocol level.

Figure 11 illustrates the protocol interaction network. It was constructed considering all the Ethereum transactions executed between January and August 2021 and filtering those directed to the set of smart contracts that can uniquely be associated with 23 known DeFi protocols.[32] Edges represent internal transactions originated by the execution of a protocol-specific smart contract, which in turn interacts with a smart contract associated with another DeFi protocol

[31] See `https://harvest-finance.gitbook.io/harvest-finance/general-info/how-to-use-1/how-to-deposit-withdraw`

[32] *0x*, *1inch*, *Balancer*, *Curvefinance*, *SushiSwap*, *UniSwap*, *Aave*, *Compound*, *Instadapp*, *MakerDAO*, *Barnbridge*, *dYdX*, *Futureswap*, *Hegic*, *Nexus*, *Syntetix*, *Badger*, *Convex*, *Fei*, *Harvestfinance*, *RenVM*, *Vesper*, *Yearn*.

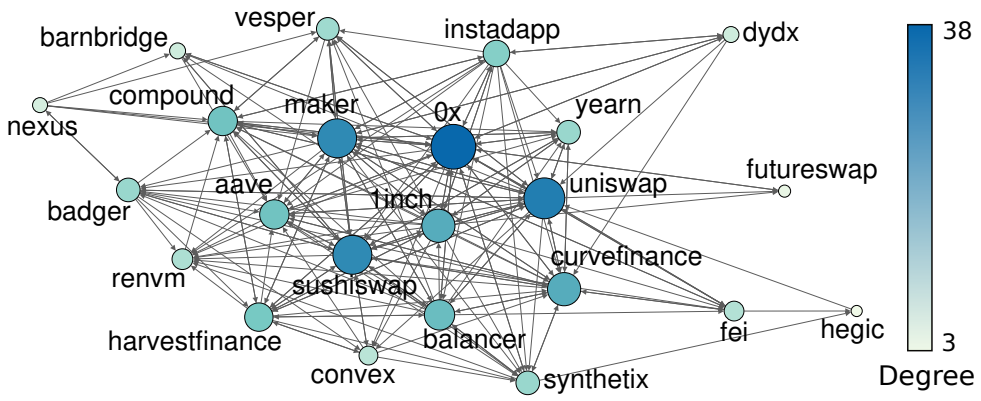

Figure 11: ***The DeFi Protocol Network.*** *The plot represents the network of DeFi protocols (nodes) and their interactions (edges). The network is constructed from a dataset of external transactions directed to a set of smart contracts manually associated with 23 DeFi protocols and the subsequent internal transactions. Nodes are constructed by aggregating all protocol-specific smart contracts, and edges represent the aggregate transactions from source protocol contracts to target protocol contracts. Edges indicate DeFi protocol interoperability. The node sizes and colors are scaled proportionally to the node degree. Nodes are highly connected. In particular, DEXs (Uniswap, Sushiswap, 0x) and lending protocols (MakerDAO, Aave) play a central role, and the aggregator 1Inch is relevant as well.*

(as in the example shown in Figure 9). Thus, edges indicate the existence of DeFi compositions. The network is highly connected: DeFi protocols heavily rely on each other.

6.4 Case Study: Assessing the Effect of Stablecoin Runs

To demonstrate the practical use of these investigation approaches, we present a case study inspired by the recent events on the Terra blockchain where we quantify to what extent a collapse of a specific stablecoin would affect the building blocks of known DeFi protocols. In May 2022, Terra was the victim of a series of trading actions that caused strong selling pressure that eventually led to the de-peg from USD, and the price of its native tokens LUNA and UST fell close to zero in a few hours [25]. The market actors sold a large amount of UST on the DEX Curve and were able to trigger a *stablecoin run* by inducing the UST holders to try and sell all their holdings in LUNA and UST. We measure to what extent a hypothetical run on two widely used stablecoins, USDC and DAI, would affect the DeFi ecosystem. We applied the building block extraction algorithm introduced in [71]. For each of the 23 DeFi protocols in our dataset, we measured the fraction of building blocks that contain one of the two tokens, either directly (within the building block itself) or indirectly (within a nested building block).

The results for DAI and USDC are reported in Figure 12, respectively in the upper and lower panels. While in many protocols the dependencies are minimal, with percentages lower than 5%, few DeFi protocols exhibit significant dependency on stablecoins: *Balancer* building blocks, for instance, heavily depend directly on both DAI (15%) and USDC (more than 30%). This means that a large fraction of all the transactions directed to such protocol might be compromised. *MakerDAO* building blocks contain both directly and indirectly DAI but not USDC, while *Instadapp* depends on both, indirectly and indirectly (with percentages up to 25%). Other protocols that exhibit significant dependency on stablecoins are *Yearn*, *Curvefinance*, and *Compound*. In summary, these results illustrate the obvious: protocols with higher exposure to these stablecoins are also those that would be more affected by potential shocks hitting the DeFi ecosystem as a consequence of stablecoin runs. However, such an investigation approach allows us to systematically assess and quantify interdependencies, which is a fundamental requirement for decision and policymakers.

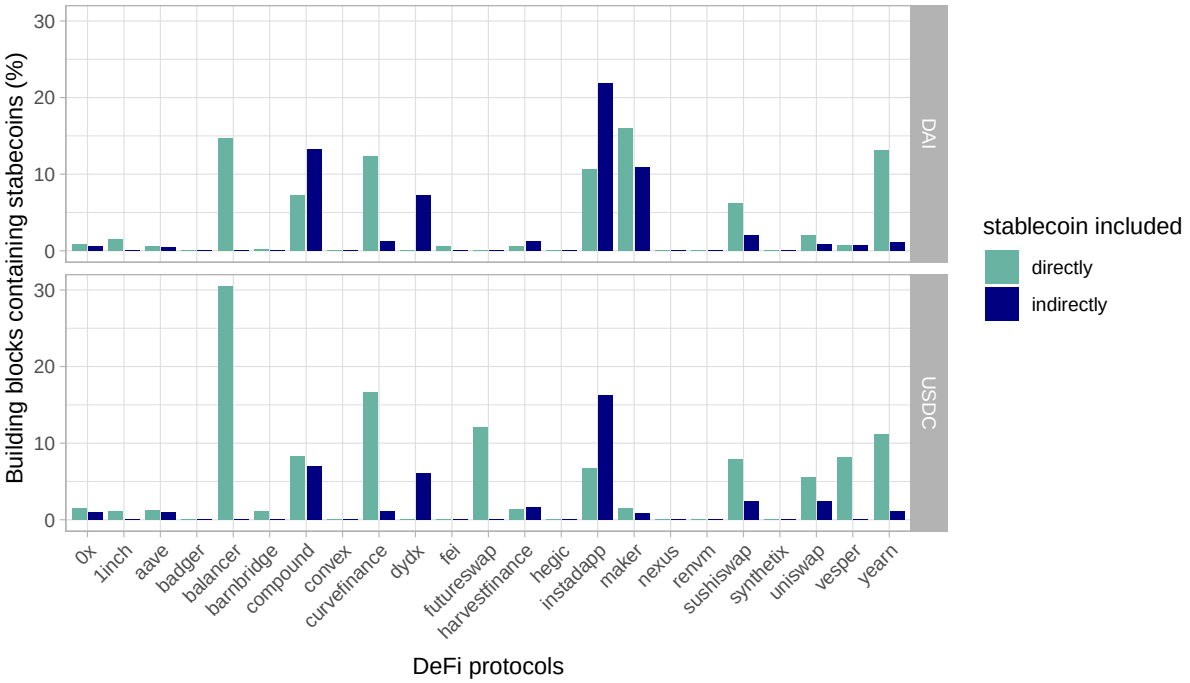

Figure 12: ***Protocol exposure to stablecoin runs***. *For each of the 23 DeFi protocols in our dataset, we measure the fraction of building blocks that are directly or indirectly dependent on DAI (top panel) and on USDC (bottom panel). While most protocols do not rely heavily on stablecoins, a few of them have significant dependencies on USDC (Balancer, Instadapp) and on DAI (Instadapp, MakerDAO, Compound).*

7 An Interdisciplinary Research Agenda

DeFi builds on non-trivial technical primitives to offer financial services that cannot directly be mapped to those provided by traditional financial institutions. We believe a deeper understanding can only be brought about by a multi-disciplinary, deeply linked research agenda. Following the DSR Model described in Section 2, we now delineate future research directions along with each stack sub-layer.

7.1 Settlement Layer

Multichain DeFi Protocols and Cross-chain Interoperability Section 3 focuses mostly on EVM-based DLTs. At the time of writing, Ethereum is still the most relevant blockchain for DeFi, with a Total Value Locked (TVL) exceeding 40 billion USD. However, many other blockchains provide similar DeFi services to those we described in the previous paragraphs. The most relevant are compatible with the Ethereum Virtual Machine.[33] They facilitate code reusability, as the same project can easily be deployed on multiple chains: for instance, all the main *1inch* smart contracts are deployed both on Ethereum and on BSC. Non-EVM compatible chains[34] typically support fewer DeFi protocols because the entry barrier for migrating existing projects is higher. We can already point to some protocols deployed on these alternative blockchains,[35] and we note that many of the protocols described in Section 5 are now moving in the direction of deploying their smart contracts in multiple DLTs (thus, we call them *multichain* protocols).

[33]Binance Smart Chain (BSC), Avalanche, Polygon, Cosmos, Cronos, Fantom, Arbitrum.

[34]Terra, Solana, Cardano, Waves, Parallel, Algorand, DeFiChain, Near, EOS.

[35]DEXs: Pancakeswap on BSC, QuickSwap on Polygon, Orca on Solana. Lending protocols: Venus on BSC, Benqi on Avalanche, Anchor on Terra. Neutrino, on Waves, is an algorithmic price-stable protocol.

The deployment of DeFi protocols on multiple chains leads to the problem that a DeFi protocol running on a separate ledger cannot communicate or call contracts of protocols deployed on another ledger. Therefore, recent efforts aim to develop solutions that enhance interoperability *across* blockchains [101]. The challenge lies in finding mechanisms that allow a source ledger to change the state of a target ledger [21].

Atomic swaps are protocols based on sequences of transactions executed on multiple DLTs that allow counterparts to coordinate on the exchange of native tokens in a trustless environment and without intermediaries [62, 117, 126]. *Bridges* are another interoperability approach. *ThorChain*, for instance, is a DeFi project that enables the swap of native assets, such as ETH and BTC, through a bridging blockchain. When such a swap occurs, BTC is sent into ThorChain Vaults, and the first trade against RUNE, the native token of ThorChain, takes place; then, a second trade is conducted from RUNE to ETH. Several DeFi protocols implemented similar bridges that enable the migration of assets across different blockchains. Furthermore, *Sidechains* [110] can be thought of as blockchains that are pegged to the main blockchain. *Polygon*, for instance, is an EVM-based scaling sidechain solution for Ethereum. Users can exploit smart contracts to lock cryptoassets in the main chain and, in turn, unlock them on the sidechain. As it is EVM-compatible, it is possible to deploy smart contracts also in the sidechain. Ronin is another example of sidechain and was built with Ethereum specifically for a popular blockchain game (Axie Infinity). Sidechains like Polygon are called "Layer 2" solutions [108].

The aforementioned solutions do not implement interoperability by default, but rather allow independent, heterogeneous blockchains to communicate. Other projects aim to provide interoperability instead as a built-in feature by implementing DLTs with a main chain and application-specific chains that can interact by design. In *Polkadot* [123], for instance, the Relay Chain plays a central role, and additional blockchains that interoperate by default, called parachains, can be created. *Cosmos* [77] implemented a similar design. It targets generic blockchain interoperability and is also based on a structure with a main blockchain, called the *hub*, and different zones that can interact with the main chain. We note that ThorChain is part of the Cosmos ecosystem.

Cross-chain interoperability has become a crucial aspect and an additional layer of complexity in DeFi. Whilst at the time of writing these solutions lead to multiple, somewhat isolated DeFi ecosystems (since smart contracts on one DLT cannot directly call contracts on another one), interoperability is more and more important, and one relevant future research direction is understanding how this aspect will affect the DeFi ecosystem.

Transaction Reordering and Mining Transaction reordering occurs when miners choose which transactions to include and how to order them when new blocks are appended to the blockchain. The profit generated by this practice is called miner extractable value (MEV). Account states are updated via transactions that trigger state transitions: thus, state updates are not independent of the order they are included in a block, and transaction ordering may affect the outcome of trading activity involving DeFi actors, for instance, by leading to unintended state updates [112]. This has implications both on miners' incentives and on the DeFi users trading activity, and from an economic perspective, these aspects can be approached using game-theoretic analysis and related methodologies. In [29], for instance, the authors exploit game theory to distinguish legitimate competition from attacks that aim at maximize MEV. Previous research [98] has shown that rational miners are incentivized to deliberately fork a blockchain, with consequences on its security, to replicate profitable transactions executed by other DeFi users in newly added blocks. They show that techniques exploiting transaction ordering such as front-, back- running and sandwitch attacks, liquidations and arbitrage actions are relevant sources of MEV. Furthermore, centralized servers called relayers put miners in direct contact with third parties that crawl the blockchain looking for MEV opportunities. The latter pay miners to order transactions as they request. The game theoretical model introduced in [31]

investigates the economic incentives behind the adoption of such services; further research in this direction is needed, in order to better understand this recent phenomenon.

7.2 Cryptoassets

Section 4 provides a taxonomy of cryptoassets. However, it is incomplete, and new standards besides ERC-20 and ERC-721 that implement additional functionalities are emerging. Further, many existing cryptoassets, and in particular tokenized assets, are typically assets that derive their price from an underlying (crypto)asset and can then be regarded as a form of derivatives. A systemization of knowledge in this sense would be beneficial, in order to identify multiple cryptoasset categories and map them to different types of derivative contracts, based on their design. Other relevant research directions relate, e.g., to portfolio choices on cryptoassets and traditional assets [28], or aim at investigating what cryptoassets and how DeFi could facilitate illicit activities [93].

7.3 DeFi Protocols

At the time of writing, relevant DeFi protocols such as Compound are launching new protocol versions based on updated smart contracts that might implement innovative financial functionalities. The figures provided in Section 5 could, therefore, become outdated soon.

Understanding the current structure and features of the DeFi protocols, as well as the new ones, is a problem that can be modeled by economists through a mechanism design approach. This might help designing protocols with desirable characteristics aiming e.g. at reaching the social optimum [30]. Generalizing the protocol mechanism designs to optimize their functioning and devise new features is also a relevant objective. Appropriate tools for modeling, simulation, and implementation are needed to reach these goals [131]. It is also essential to devise financial models that allow for mitigating financial risk associated with existing protocols, and to adapt well-known methodologies from traditional finance to the innovative protocol designs of DeFi protocols [58]. There is, however, a problem in applying mechanism design to blockchain, as the "designer" can create its own tokens. This is not a possibility usually considered in standard microeconomic theory, which limits the applicability of the standard mechanism design results to blockchain; a model to overcome this limitation in the case of auctions is proposed in [28].

Another relevant aspect that should be investigated in greater detail regards how the governance of DeFi protocols is managed and how this affects centralization [56]. Strictly related to this is the role of the entities that develop and are behind the DeFi projects. Even if such organizations manage large amounts of customer funds, they still seem to be run by small groups of individuals, as the FTX collapse showed, and little is known about who is responsible for their projects. A promising direction in this sense is, e.g., to compare whether the relative protocol size in the DeFi ecosystem translates to their organization size, and to analyze the governance token distributions across DeFi actors.

Finally, DeFi protocols are still a niche phenomenon if compared to traditional finance. It is important to understand the extent to which DeFi can be democratized to a broader audience. Surveys to understand how the public perceives the DeFi ecosystem, including what are the common misconceptions and whether DeFi is perceived positively, or to better understand what are the profiles of the investors and why are they turning to DeFi, would be greatly beneficial. Concurrently, it is essential to assess to which extent investment fraudsters exploit DeFi in comparison to other potential channels, and to investigate whether the risks for DeFi users are different from those faced by users that invest more generally in cryptocurrencies.

7.4 DeFi Composability

Section 6 describes how composability has emerged as a relevant aspect of the DeFi ecosystem. Analyzing DeFi protocol interdependencies is just the initial step in a more comprehensive sys-

temic risk assessment. Previous studies have shown, for instance, that given certain market conditions, DeFi protocols that exploit over-collateralization might suffer from drying-up liquidity issues and become insolvent [59]. Also, repeatedly tokenized assets can create dependencies across DeFi actors [118] and raise stability concerns. Future research should focus on understanding systemic risk more profoundly, for instance by analyzing token flows [70] and protocol dependencies, both within the crypto-ecosystem and by considering the potential spillovers from and to the traditional financial system [41, 83]. Future research should also pay particular attention on whether and in case how to further integrate DeFi in Fintech and in the traditional financial ecosystem.

8 Conclusions

We systematized the technical primitives and financial functionalities provided by DeFi protocols. We started by describing the underlying technical primitives. Then, we outlined the various types of cryptoassets used in DeFi and focused on specific DeFi protocol categories providing financial services such as exchanging or lending and borrowing cryptoassets to economic agents. Next, we described how DeFi protocols could be assembled into complex financial constructs through compositions. We also pointed out possible investigation and measurement methods that could be applied to disentangle the building blocks of DeFi protocols or study the network structure of the broader DeFi ecosystem. To illustrate the practical applicability of these methods, we showed how a stablecoin run could affect other DeFi protocols. Finally, we provide pointers on future research directions that could help to understand DeFi protocols and their ecosystems, such as protocol dependencies and smart contract composability, in a comprehensive systemic risk assessment and the investigation of interoperability aspects across DLTs.

DeFi integrates technical, financial, and socio-economic complexity in an unprecedented way. This development could be neglected while DeFi was still a niche phenomenon without ties to the fiat system. However, with the increasing integration of cryptoassets with the traditional financial sector, we require novel methods to identify, investigate, and ultimately understand the risks associated with these developments. The scientific method embedded in a multi-disciplinary setting offers the most promising answer to this challenge.

References

[1] Aave. Protocol whitepaper. Technical report, 2020. Available at `https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf`.

[2] Hayden Adams. Uniswap v1 whitepaper. Technical report, 2019. Available at `https://hackmd.io/@HaydenAdams/HJ9jLsfTz`.

[3] Hayden Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core. Technical report, 2021. Available at `https://uniswap.org/whitepaper.pdf`.

[4] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. Technical report, 2021. Available at `https://uniswap.org/whitepaper-v3.pdf`.

[5] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, AFT '20, pages 80–91. Association for Computing Machinery, 2020.

[6] Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and Tarun Chitra. An analysis of uniswap markets. *Cryptoeconomic Systems*, 0(1), 2021.

[7] Thomas Ankenbrand, Denis Bieri, Roland Cortivo, Johannes Hoehener, and Thomas Hardjono. Proposal for a comprehensive (crypto) asset taxonomy. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 16–26. IEEE, 2020.

[8] Matteo Aquilina, Jon Frost, and Andreas Schrimpf. The rationale for regulation of defi: a functional approach. Technical report, 2022.

[9] Sirio Aramonte, Sebastian Doerr, Wenqian Huang, Andreas Schrimpf, et al. Defi lending: intermediation without information? Tech. rep., Bank for International Settlements, 2022.

[10] Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf. Defi risks and the decentralisation illusion. *BIS Quarterly Review*, page 21, 2021.

[11] Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli, Stefano Lande, and Roberto Zunino. Sok: Unraveling bitcoin smart contracts. In *International Conference on Principles of Security and Trust*, pages 217–242. Springer, 2018.

[12] Raphael Auer. Beyond the doomsday economics of "proof-of-work" in cryptocurrencies. Bank for International Settlements Working Papers 765, 2019.

[13] Raphael Auer, Marc Farag, Ulf Lewrick, Lovrenc Orazem, and Markus Zoss. Banking in the shadow of bitcoin? the institutional adoption of cryptocurrencies. Bank for International Settlements Working Papers 1013, 2022.

[14] Raphael Auer, Jon Frost, and Jose María Vidal Pastor. Miners as intermediaries: extractable value and market manipulation in crypto and defi. Bank for International Settlements Bulletins 58, 2022.

[15] Raphael Auer, Cyril Monnet, and Hyun Song Shin. Distributed ledgers and the governance of money. Bank for International Settlements Working Papers 924, 2022.

[16] Badger. Gitbook. Technical report, 2022. Available at `https://docs.badger.com/`.

[17] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger, and Gilbert Fridgen. Defi, not so decentralized: The measured distribution of voting rights. In *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022.

[18] Barnbridge. Barnbridge - a fluctuations derivatives protocol for hedging yield sensitivity and market price. Technical report, 2021. Available at `https://github.com/BarnBridge/BarnBridge-Whitepaper`.

[19] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. Sok: lending pools in decentralized finance. In *International Conference on Financial Cryptography and Data Security*, pages 553–578. Springer, 2021.

[20] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. A theory of automated market makers in defi. In *International Conference on Coordination Languages and Models*, pages 168–187. Springer, 2021.

[21] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8):1–41, 2021.

[22] BIS. A glossary of terms used in payments and settlement systems. Technical report, Bank for International Settlements, 2003.

[23] BIS. Annual economic report. chapter 3: The future monetary system. Technical report, Bank for International Settlements, June 2022.

[24] BIS. Bis and central banks of france, singapore and switzerland to explore cross-border cbdc trading and settlement using defi protocols. Technical report, Bank for International Settlements, November 2022.

[25] Antonio Briola, David Vidal-Tomás, Yuanrong Wang, and Tomaso Aste. Anatomy of a stablecoin's failure: The terra-luna case. *Finance Research Letters*, 51:103358, 2023.

[26] Investor Protection Bureau. Attorney general james ends virtual currency trading platform bitfinex's illegal activities in new york. Available at `https://on.ny.gov/3izikSX`, 2021.

[27] Giulio Caldarelli. Wrapping trust for interoperability: A preliminary study of wrapped tokens. *Information*, 13(1):6, 2022.

[28] Andrea Canidio. Auctions with tokens, 2022. Available at: `https://www.dropbox.com/s/dksejx5h7sye2ms/Canidio-Auctions-with-tokens.pdf?dl=0`.

[29] Andrea Canidio and Vincent Danos. Commitment against front running attacks, 2022. Available at: `https://www.dropbox.com/s/pmketrifnnfv2nu/Canidio-Danos-front-running.pdf?dl=0`.

[30] Agostino Capponi and Ruizhe Jia. The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*, 2021.

[31] Agostino Capponi, Ruizhe Jia, and Ye Wang. The evolution of blockchain: from lit to dark. *arXiv preprint arXiv:2202.05779*, 2022.

[32] Nic Carter and Linda Jeng. Defi protocol risks: The paradox of defi, 2021. Chapter of "Regtech, Suptech and Beyond: Innovation and Technology in Financial Services", RiskBooks.

[33] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[34] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Comput. Surv.*, 53(3):1–43, jun 2020.

[35] Ting Chen, Zihao Li, Yufei Zhang, Xiapu Luo, Ang Chen, Kun Yang, Bin Hu, Tong Zhu, Shifang Deng, Teng Hu, et al. Dataether: Data exploration framework for ethereum. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 1369–1380. IEEE, 2019.

[36] Simon Cousaert, Jiahua Xu, and Toshiko Matsui. Sok: Yield aggregators in defi. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–14. IEEE, 2022.

[37] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. IEEE, 2020.

[38] Alpha Venture DAO. Alpha homora v2. Technical report, 2021. Available at `https://github.com/AlphaFinanceLab/alpha-homora-v2-contract`.

[39] Alex de Vries. Bitcoin boom: What rising prices mean for the network's energy consumption. *Joule*, 5(3):509–513, 2021.

[40] DeFiLama, 2022. Available at: `https://defillama.com/`.

[41] Christian Diem, Anton Pichler, and Stefan Thurner. What is the minimal systemic risk in financial exposure networks? *Journal of Economic Dynamics and Control*, 116:103900, 2020.

[42] Anil Donmez and Alexander Karaivanov. Transaction fee economics in the ethereum blockchain. *Economic Inquiry*, 60(1):265–292, 2022.

[43] Nabil El Ioini and Claus Pahl. A review of distributed ledger technologies. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*, pages 277–288. Springer, 2018.

[44] Daniel Engel and Maurice Herlihy. Composing networks of automated market makers. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, pages 15–28, 2021.

[45] Etherdelta. Etherdelta protocol, 2022. Available at `https://etherdelta.com/`.

[46] Ethereum. The ethereum merge, 2022. Available at `https://ethmerge.com/`.

[47] European Banking Authority. Eba reports on crypto-assets, 2019. Available at `https://www.eba.europa.eu/eba-reports-on-crypto-assets`.

[48] Alex Evans. Liquidity provider returns in geometric mean markets. *Cryptoeconomic Systems*, 1(2), 2021.

[49] Alex Evans, Guillermo Angeris, and Tarun Chitra. Optimal fees for geometric mean market makers. In *International Conference on Financial Cryptography and Data Security*, pages 65–79. Springer, 2021.

[50] Sizheng Fan, Tian Min, Xiao Wu, and Cai Wei. Towards understanding governance tokens in liquidity mining: a case study of decentralized exchanges. *World Wide Web*, 2022.

[51] Harvest Finance. Harvest finance protocol. Technical report, 2022. Available at `https://harvest-finance.gitbook.io/harvest-finance/`.

[52] Idle Finance. Documentation. Tech. rep., 2022. See `https://docs.idle.finance/`.

[53] Pickle Finance. Documentation. Tech. rep., 2022. See https://docs.pickle.finance/.

[54] Yearn Finance. Yearn finance 3 - decentralized finance. Technical report, 2020. Available at https://www.allcryptowhitepapers.com/wp-content/uploads/2020/12/YFI3.pdf.

[55] Robin Fritsch, Samuel Käser, and Roger Wattenhofer. The economics of automated market makers. *arXiv preprint arXiv:2206.04634*, 2022.

[56] Michael Froewis, Kiran Sridhar, Christos Makridis, and Rainer Böhme. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Available at SSRN 3915140*, 2021.

[57] FSB. Assessment of risks to financial stability from crypto-assets. Technical report, Financial Stability Board, 2022.

[58] Masaaki Fukasawa, Basile Maire, and Marcus Wunsch. Weighted variance swaps hedge against impermanent loss. *Available at SSRN 4095029*, 2022.

[59] Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15. IEEE, 2020.

[60] Lewis Gudgeon, Sam Werner, Daniel Perez, and William J Knottenbelt. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 92–112, 2020.

[61] Campell R. Harvey, Ashwin Ramachandran, and Joey Santoro. *DeFi and the Future of Finance*. John Wiley & Sons, 2021.

[62] Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254, 2018.

[63] Eyal Hertzog, Guy Benartzi, and Galia Benartzi. Bancor protocol. Technical report, 2017. Available at https://cryptopapers.info/assets/pdf/bancor.pdf.

[64] Marco Huber and Vinzenz Treytl. Risks in defi-lending protocols-an exploratory categorization and analysis of interest rate differences. In *International Conference on Database and Expert Systems Applications*, pages 258–269. Springer, 2022.

[65] IMF. Global financial stability report: October 2021. Technical report, International Monetary Fund, 2021.

[66] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions. *arXiv preprint arXiv:2102.10096*, 2021.

[67] Antonio Juliano. dydx: A standard for decentralized margin trading and derivatives. Technical report, 2018. Available at https://whitepaper.dydx.exchange/.

[68] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. An analysis of the market risk to participants in the compound protocol. In *Third International Symposium on Foundations and Applications of Blockchains*, 2020.

[69] Hugh Karp and Reinis Melbardis. Nexus mutual - a peer-to-peer discretionary mutual on the ethereum blockchain. Technical report, 2022. Available at https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf.

[70] Stefan Kitzler, Christian Diem, Pietro Saggese, Bernhard Haslhofer, and Stefan Thurner. Systemic risk in decentralized finance (defi) - an investigation of smart contract interdependencies. In *11th International Conference on Complex Networks and Their Applications*, 2022.

[71] Stefan Kitzler, Friedhelm Victor, Pietro Saggese, and Bernhard Haslhofer. Disentangling decentralized finance (defi) compositions. *ACM Trans. Web*, oct 2022.

[72] Stefan Kitzler, Friedhelm Victor, Pietro Saggese, and Bernhard Haslhofer. A systematic investigation of defi compositions in ethereum. In *The 2nd Workshop on DeFi, International Conference on Financial Cryptography and Data Security*, 2022.

[73] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 59–79, 2020.

[74] Ariah Klages-Mundt and Andreea Minca. (In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. *Cryptoeconomic Systems*, 1(2), oct 2021.

[75] Bhaskar Krishnamachari, Qi Feng, and Eugenio Grippo. Dynamic curves for decentralized autonomous cryptocurrency exchanges. *arXiv preprint arXiv:2101.02778*, 2021.

[76] Sumit Kumar. Central clearing of crypto-derivatives in a decentralized finance (defi) framework: An exploratory review. *International Journal of Business and Economics*, 7(1):128, 2022.

[77] Jae Kwon and Ethan Buchman. Cosmos whitepaper. *A Netw. Distrib. Ledgers*, 2019.

[78] Robert Lauko and Richard Pardoe. Liquity: decentralized borrowing protocol. Technical report, 2021. Available at `https://docsend.com/view/bwiczmy`.

[79] Jens Lausen. Regulating initial coin offerings? a taxonomy of crypto-assets. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, 2019.

[80] Alfred Lehar and Christine A Parlour. Decentralized exchanges. *Available at SSRN 3905316*, 2021.

[81] Robert Leshner and Geoffrey Hayes. Compound: The money market protocol. Technical report, 2019. Available at `https://bit.ly/3ioWOjW`.

[82] Lindsay X Lin. Deconstructing decentralized exchanges. *Stan. J. Blockchain L. & Pol'y*, 2:58, 2019.

[83] Peter Lindner, Axel Loeffler, Esther Segalla, Guzel Valitova, and Ursula Vogel. International monetary policy spillovers through the bank funding channel. *Journal of International Money and Finance*, 90:161–174, 2019.

[84] Guilherme Maia and João Vieira dos Santos. Mica and defi ('proposal for a regulation on market in crypto-assets' and 'decentralised finance'). *Available at SSRN 3875355*, 2021.

[85] MakerDAO. The maker protocol: Makerdao's multi-collateral dai (mcd) system. Technical report, 2020. Available at `https://makerdao.com/en/whitepaper`.

[86] Fernando Martinelli and Nikolai Mushegian. Balancer: a non-custodial portfolio manager, liquidity provider, and price sensor. Technical report, 2019. Available at `https://balancer.fi/whitepaper.pdf`.

[87] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. Sok: A classification framework for stablecoin designs. In *International Conference on Financial Cryptography and Data Security*, pages 174–197. Springer, 2020.

[88] Matthieu Nadini, Laura Alessandretti, Flavio Di Giacinto, Mauro Martino, Luca Maria Aiello, and Andrea Baronchelli. Mapping the nft revolution: market trends, trade networks, and visual features. *Scientific reports*, 11(1):1–11, 2021.

[89] Danny Nelson and Tracy Wang. Master of anons: How a crypto developer faked a defi ecosystem. Available at: `https://www.coindesk.com/layer2/2022/08/04/master-of-anons-how-a-crypto-developer-faked-a-defi-ecosystem/`.

[90] Lucas Nuzzi, Antoine Le Calvez, and Kyle Waters. Understanding total value locked (tvl), 2021. Available at: `https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-0c0`.

[91] Karl J. O'Dwyer and David Malone. Bitcoin mining and its energy footprint. In *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014 CIICT 2014)*, pages 280–285, 2014.

[92] Luis Oliveira, Liudmila Zavolokina, Ingrid Bauer, and Gerhard Schwabe. To token or not to token: Tools for understanding blockchain tokens. In *International Conference of Information Systems (ICIS 2018)*, San Francisco, USA, December 2018. ICIS.

[93] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoit Dupont. Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1), 2019.

[94] Daniel Perez, Sam M Werner, Jiahua Xu, and Benjamin Livshits. Liquidations: Defi on a knife-edge. In *International Conference on Financial Cryptography and Data Security*, pages 457–476. Springer, 2021.

[95] Andrei-Dragos Popescu. Transitions and concepts within decentralized finance (defi) space. *Research Terminals in the social sciences*, 2020.

[96] Curve protocol. Curve documentation. Technical report, 2022. Available at `https://curve.readthedocs.io/_/downloads/en/latest/pdf/`.

[97] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. An empirical study of defi liquidations: Incentives, risks, and instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*, 2021.

[98] Kaihua Qin, Liyi Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 198–214. IEEE, 2022.

[99] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the defi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security*, pages 3–32. Springer, 2021.

[100] Rahul Rai. The death spiral: How terra's algorithmic stablecoin came crashing down, 2022. Available at: `https://www.forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down/?sh=41275c6a71a2`.

[101] Peter Robinson. Survey of crosschain communications protocols. *Computer Networks*, 200, 2021.

[102] Meni Rosenfeld et al. Overview of colored coins, white paper. *bitcoil. co. il*, 41:94, 2012.

[103] Kanis Saengchote. Decentralized lending and its users: Insights from compound. *Available at SSRN 3925344*, 2022.

[104] Mehdi Salehi, Jeremy Clark, and Mohammad Mannan. Red-black coins: Dai without liquidations. In *International Conference on Financial Cryptography and Data Security*, pages 136–145. Springer, 2021.

[105] Joey Santoro. Fei protocol: A decentralized, fair, liquid, and scalable stablecoin platform. Tech. rep., 2021. Available at `https://assets.fei.money/docs/whitepaper.pdf`.

[106] George Sazandrishvili. Asset tokenization in plain english. *Journal of Corporate Accounting & Finance*, 31(2):68–73, 2020.

[107] Fabian Schär. Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 2:153–74, 2021.

[108] Cosimo Sguanci, Roberto Spatafora, and Andrea Mario Vergani. Layer 2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*, 2021.

[109] Hyun Song Shin. The great crypto crisis is upon us. Available at `https://www.ft.com/content/76234c49-cb11-4c2a-9a80-49da4f0ad7dd`.

[110] Amritraj Singh, Kelly Click, Reza M Parizi, Qi Zhang, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149, 2020.

[111] Kyle Soska, Jin-Dong Dong, Alex Khodaverdian, Ariel Zetlin-Jones, Bryan Routledge, and Nicolas Christin. Towards understanding cryptocurrency derivatives: A case study of bitmex. In *Proceedings of the Web Conference 2021 (WWW '21)*, 4 2021.

[112] Nicholas Stifter, Aljosha Judmayer, Philipp Schindler, and Edgar Weippl. Opportunistic algorithmic double-spending: How i learned to stop worrying and love the fork. In *Computer Security – ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part I*, pages 46–66, Berlin, Heidelberg, 2022. Springer-Verlag.

[113] Katerina Stroponiati, Ilya Abugov, Yiannis Varelas, Kostas Stroponiatis, Modesta Jurgeleviciene, and Yashoda Savanth. Decentralized governance in defi: Examples and pitfalls. Technical report, DappRadar, 2020.

[114] Sushiswap. Documentation. Tech. rep., 2022. Available at `https://docs.sushi.com/`.

[115] Synthetix. Synthetix litepaper. Technical report, 2022. Available at `https://docs.synthetix.io/litepaper/`.

[116] Palina Tolmach, Yi Li, Shang-Wei Lin, and Yang Liu. Formal analysis of composable defi protocols. In *International Conference on Financial Cryptography and Data Security*, pages 149–161. Springer, 2021.

[117] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. Mad-htlc: because htlc is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1230–1248. IEEE, 2021.

[118] Victor von Wachter, Johannes Rude Jensen, and Omri Ross. Measuring asset composability as a proxy for defi integration. In *International Conference on Financial Cryptography and Data Security*, pages 109–114. Springer, 2021.

[119] Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. Cyclic arbitrage in decentralized exchanges. In *Companion Proceedings of the Web Conference 2022*, WWW '22, pages 12–19. Association for Computing Machinery, 2022.

[120] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain. Technical report, 2017. Available at: `https://github.com/0xProject/whitepaper/blob/master/0x_white_paper.pdf`.

[121] Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778*, 2021.

[122] Molly Wintermute. Hegic: On-chain options trading protocol on ethereum powered by hedge contracts and liquidity pools. Technical report, 2020. Available at `https://creb aco.com/planner/admin/uploads/whitepapers/5261261Hegic.pdf`.

[123] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. Technical report, 2016. Available at `https://polkadot.network/PolkaDotPaper.pdf`.

[124] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[125] Yang Xiao, Ning Zhang, Wenjing Lou, and Y Thomas Hou. A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2):1432–1465, 2020.

[126] Jiahua Xu, Damien Ackerer, and Alevtina Dubovitskaya. A game-theoretic analysis of cross-chain atomic swaps with htlcs. In *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, pages 584–594. IEEE, 2021.

[127] Jiahua Xu and Yebo Feng. Reap the harvest on blockchain: A survey of yield farming protocols. *IEEE Transactions on Network and Service Management*, 2022.

[128] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols. *ACM Comput. Surv.*, 2022.

[129] Jiahua Xu and Nikhil Vadgama. From banks to defi: the evolution of the lending market. In *Enabling the Internet of Value*, pages 53–66. Springer, 2022.

[130] Teng Andrea Xu and Jiahua Xu. A short survey on business models of decentralized finance (defi) protocols. *arXiv preprint arXiv:2202.07742*, 2022.

[131] Michael Zargham, Jamsheed Shorish, and Krzysztof Paruch. From curved bonding to configuration spaces. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3. IEEE, 2020.

[132] Shijie Zhang and Jong-Hyouk Lee. Analysis of the main consensus protocols of blockchain. *ICT express*, 6(2):93–97, 2020.

[133] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. Sok: Decentralized finance (defi) attacks. Cryptology ePrint Archive, Paper 2022/1773, 2022. `https://eprint.iacr.org/2022/1773`.