Digital Finance (2024) 6:55–95
https://doi.org/10.1007/s42521-023-00088-8

ORIGINAL ARTICLE

The technology of decentralized finance (DeFi)

Raphael Auer[1] · Bernhard Haslhofer[2] · Stefan Kitzler[3] · Pietro Saggese[3] · Friedhelm Victor[4]

Received: 10 March 2023 / Accepted: 21 June 2023 / Published online: 1 August 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 traditional centralized intermediaries. A range of DeFi protocols implements these services as a suite of smart contracts, i.e., software programs that encode the logic of conventional financial operations. Instead of transacting with a counterparty, DeFi users interact with software programs that pool the resources of other DeFi users. DeFi's programmable and automated technology could foster efficiency and increase transparency. However, it exposes users to idiosyncratic risks, such as smart contract vulnerabilities and complex protocol interoperability. This paper provides a deep dive into the overall architecture, the technical primitives, and the financial functionalities of DeFi protocols. We analyze 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, i.e., decentralized exchanges, lending protocols, derivatives protocols and aggregators. The latter exploit the property that smart contracts can be "composed," i.e., 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 Decentralized finance · DeFi · Blockchain · Ethereum · DLT · Stablecoin · Cryptoasset

JEL Classification E42 · E58 · F31 · G19 · G23 · L50 · O33 · G12

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.

Extended author information available on the last page of the article

1 Introduction

Decentralized Finance (DeFi) offers on-chain financial services such as borrowing, lending, or investing without relying on a traditional centralized financial intermediary (Werner et al., 2021). DeFi applications strive for disintermediation and censorship resistance, with partial success (Carter & Jeng, 2021; Donmez & Karaivanov, 2022). They are often realized as open-source software and enable governance models that let arbitrary stakeholders participate in decision-making processes (Jensen et al., 2021). Technically, such services are implemented as executable software programs called *smart contracts* of which execution is automated, ensuring deterministic outcomes and reusability. These programs are then deployed on smart contract-enabling distributed ledger technologies (DLTs) such as Ethereum (Wood et al., 2014) or Solana. Interest in DeFi rose sharply in 2020, and the Total Value Locked (TVL) is now relatively stable at around 50 billion USD (DeFiLama, 2022), after a peak of 150 billion USD in 2021.[1]

It is still unclear if and to what extent DeFi will proliferate in the future (BIS, 2022a). Today, cryptoasset trading happens mostly off-chain on centralized crypto exchanges, which does not constitute DeFi (Aramonte et al., 2021; Auer et al., 2022). Recent episodes of market turmoil have led to a discussion on whether and how the DeFi industry should be regulated (Aquilina et al., 2022; Shin, 2022).

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 cryptoasset 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, or the potential automation of contract settlements that currently require extensive manual work. 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 (Harvey, 2021).

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 (Kitzler et al., 2022c). 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, embedded in the current markets for a programmable financial ecosystem (BIS, 2022a). One example in this direction is Project Mariana of the BIS Innovation Hub, the Eurosystem's Banque de France, the

[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. Nelson and Wang (2022); Nuzzi et al. (2021)).

Monetary Authority of Singapore, and the Swiss National Bank, which examines the role of automated market makers in foreign exchange markets (BIS, 2022b).

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., Aramonte et al., 2021; FSB, 2022). DeFi is subject to risks common to the broader financial system: lending protocols can become insufficiently collateralized or insolvent (Gudgeon et al., 2020). Furthermore, the promises of transparency and stability in DeFi are not necessarily guaranteed, as is exemplified by investigations into the stablecoin Tether (Investor Protection Bureau, 2021). A stablecoin run with consequent deleveraging spiral effects (Briola et al., 2023; Klages-Mundt & Minca, 2021) 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 (Rai, 2022). Similarly, after the bankruptcy of the Silicon Valley Bank, the stablecoin USDC lost its peg to the US dollar as Circle, the company behind USDC, held $3.3 billion worth of reserves at SVB.[2] DeFi is also subject to novel, specific risks such as smart contracts vulnerabilities, which can expose them to hacks or exploits (Chen et al., 2020). New governance models may distribute and democratize decision-making power by tokenizing voting rights; however, voting rights are highly concentrated (Barbereau et al., 2023) and malicious users can purchase the majority of tokens to manipulate protocols (Twitter, 2021). Oracles, that feed external information such as real-world asset prices into the distributed ledger technology, are also vulnerable to manipulation (Mackinga et al., 2022). Miners and validators can choose which transactions they add to the ledger and in which order, giving rise to the prevalence of front-running and related issues (Auer et al., 2022). The rise of DeFi has been accompanied by many incidents with an accumulated total loss exceeding 3 billion USD (Zhou et al., 2022). These incidents highlight the risks of technical vulnerabilities and their amplification caused by the intertwined nature of DeFi (Kitzler et al., 2022c).

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, with this paper we aim to introduce a broader audience having diverse backgrounds to the technical primitives and financial functions of DeFi and its protocols, by including the most recent findings that shed light on their functioning, design, and on how they interoperate. This study contributes to the literature that describes DeFi as a layered stack (Chen et al., 2020; Schär, 2021; Werner et al., 2021; Zhou et al., 2022). We provide a clear distinction between the technical and the financial DeFi fundamentals (Harvey, 2021), and identify the layers to which they are associated. We incorporate recent advancements that expand prior knowledge on the compositions of financial DeFi services and include an additional layer for end-user interactions. We utilize transaction-based sequence diagrams to describe the interactions between economic agents and DeFi protocols. Based on that, we introduce the

[2] See e.g. https://www.ft.com/content/7c9b2234-c298-4508-b59a-fce49f6bc40a.

peer-to-pool model, that generalizes the economic incentives of DeFi users across protocols.

Building on previous work, we introduce the DeFi Stack Reference (DSR) model in Sect. 2 as a conceptualization of the technical primitives and financial functions that DeFi protocols build upon. Then, in Sect. 3, we describe in more detail the essential technical primitives, such as DLTs and smart contracts. Next, in Sect. 4, we outline the spectrum of cryptoassets used to represent and transfer value in the DeFi ecosystem. In Sect. 5, we describe the design and financial functions of the most prominent DeFi protocol families and abstract them into a generalized DeFi framework. After focusing on individual DeFi protocols, we describe how they can be combined into DeFi compositions (Sect. 6). Finally, in Sect. 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 miners, or validators, compete to process and settle transactions. Users can choose from different financial protocols; these are contestable as anyone can deploy a new protocol, fork[3] the source code of an existing one, 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 DLT 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

[3] i.e., copy. Source code of DeFi protocols is typically open source.

subecosystem, both in terms of value locked and relevance of financial protocols built on top of it.

We also note that only "on-chain"[4] financial activity can be categorized as DeFi. Cryptoasset exchanges such as the recently collapsed FTX[5] 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 loan companies like Celsius[6] 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. 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, also interacting with a smart contract. In return for contributing liquidity, lenders receive an equity token that tracks ownership of the lent asset. 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, i.e., 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. Building on earlier research that introduced a layered stack framework for DeFi (Chen et al., 2020; Schär, 2021; Werner et al., 2021; Zhou et al., 2022), and considering new developments, we introduce a DeFi Stack Reference (DSR) Model to illustrate the technical primitives, financial functions, and compositions of DeFi protocols conceptually. As shown in Fig. 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 (BIS, 2003). 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,

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

[5] See https://on.ft.com/3VG2Mw0 on the FTX failure.

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

but are embedded in the settlement layer[7] 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, decentralized exchanges (DEXs), and derivatives protocols.[8] 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 novel type of DeFi protocols, also implemented by a set of smart contracts, that by design require to interact with financial services offered by other DeFi protocols to provide their financial services. For instance, DEX Aggregators look for the best offered price for the swap of a cryptoasset pair across multiple DEXs and redirect users programmatically towards the DEX offering the best price. For comparison, all financial services provided by DEXs do not need any other protocol to operate. Yield Aggregators implement strategies to invest user funds in other DeFi protocols and maximize their returns. Aggregators are also known as Asset Management 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. It is possible to divide them into APIs, that provide programming interfaces, and UIs, that provide graphical user interfaces. They are a major component of what is referred to as the Web 3.0, i.e., the envisioned concept of a decentralized web, empowered by DLT technology to allow the exchange of value, and whose users can control their online data and identity (Wood et al., 2023). 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.

[7] E.g., they are used to pay the transaction costs, called *gas fees* in Ethereum.

[8] This category also includes protocols that offer insurance services.

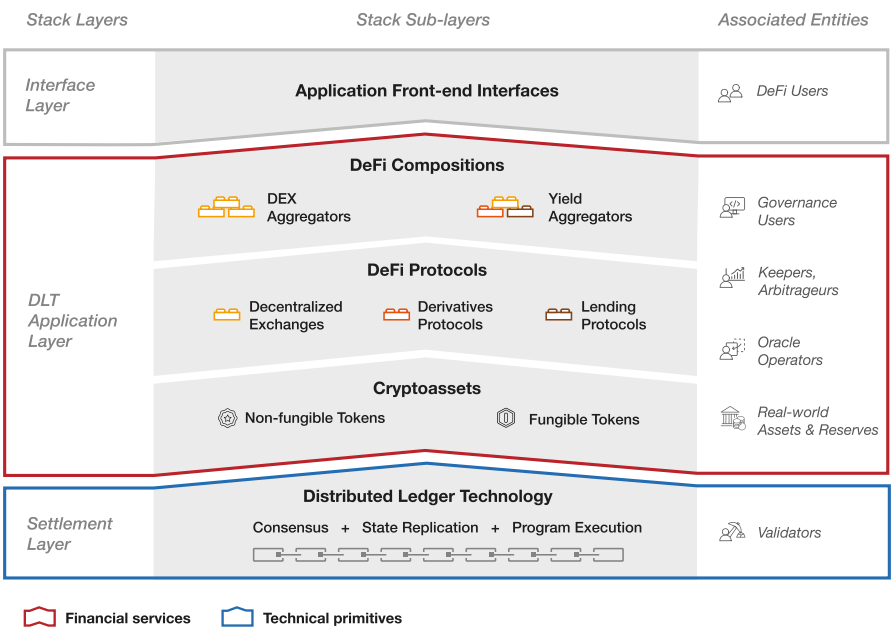

Fig. 1 DeFi stack reference (DSR) model. At the foundation, the settlement layer, DLTs allow to reach an agreement on the global state of the system, replicate it across network nodes, and execute computer programs that facilitate financial transactions in return for some native token. The DLT application 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. The interface layer provides 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

Each of these DeFi stack layers is associated with real-world entities in a broader ecosystem (see Fig. 1, right-hand side column). On the lowest layer, validators are economically incentivized to process transactions and execute programs. They can be seen as a novel form of intermediary as they verify transactions and update the DLT (Auer et al., 2022). On the application layer, keepers and arbitrageurs play a relevant role as they enforce incentive mechanisms, while governance users have decision powers through voting on protocol changes. Furthermore, 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. Cryptoassets known as stablecoins use real-world assets such as fiat currencies as a reserve. Finally, on the highest layer, end-users can interact with a DeFi application via user interfaces.

3 Settlement layer: the technical primitives

DeFi protocols run on DeFi-enabling distributed ledger technology: we, thus, begin by delving into the technical fundamentals they rely on.

Distributed Ledger Technology DLTs provide transaction execution capabilities and implement consensus protocols to agree, represent and replicate system states globally without relying on a single intermediary node (El Ioini & Pahl, 2018). Two main DLT models exist: the Bitcoin-like Unspent Transaction Output (UTXO) model and the Ethereum-like account model. In Bitcoin, UTXOs represent discrete amounts of bitcoins that can only be spent by the entity that can prove their ownership, and there is no concept of accounts or wallets on the protocol level. Instead, in the latter, the state of an account corresponds to its balance and other features such as the number of transactions sent. Transactions update the states of the accounts.

A key feature determining whether a DLT is suitable for DeFi is the availability of an execution environment for deploying and running smart contracts, i.e., software programs implementing financial functions. While the Bitcoin blockchain already provides basic mechanisms for executing custom code, its capabilities are limited (Atzei et al., 2018). 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 (Donmez & Karaivanov, 2022) caused by the increasing transaction volume. 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., Solana, Algorand, Cardano) blockchains.[9] Therefore, to date 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.

Another relevant property provided by the DLT is finality.[10] We mention in this regard an important difference between so-called 'Layer 1' and 'Layer 2' solutions. The former refers to the main DLT architecture that serves as the foundation of the settlement layer. The latter is an additional network that can be implemented on top of the underlying DLT, to provide scalability. Several different Layer 2 solutions exist. They enable users to conduct a batch of transactions off-chain so that only the final state is recorded on-chain, having important implications in terms of finality and transaction settlement. They are categorized into payment and state channels, commit chains, and protocols for refereed delegation (Gudgeon et al., 2020).

[9] See https://defillama.com/chains. EVM-compatible DLTs utilize the EVM, or a comparable execution environment, for smart contract execution. Non-EVM compatible are DLTs that are also based on the deployment of smart contracts, but utilizing a different execution environment, and their technical implementation can vary. Algorand for instance uses a different programming language and a different virtual machine with respect to Ethereum (see https://bit.ly/42Ol8xB).

[10] Time to finality can vary significantly across DLTs. See e.g., https://bit.ly/3MG2Bxw.

State Representation: Accounts As an *account-based* distributed ledger, Ethereum addresses identify an account whose state (i.e., roughly, its balance) 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 Fig. 2 shows, two different types of accounts exist: Externally Owned Accounts (EOAs), i.e., user accounts, and Contract Accounts (CAs), commonly known as 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* (Chen et al., 2019).

State Transition: Transactions 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.[11] 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 contract invocation represented on the right side of Fig. 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 recorded on the blockchain as new transactions.

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 (Xiao et al., 2020). In the DLT context, consensus

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

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 (Castro & Liskov, 2002).[12]

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the most common consensus algorithms (Zhang & Lee, 2020). Bitcoin, for instance, relies on PoW. Miners must conduct computationally intensive tasks to participate in the process of adding new transactions to the blockchain (and earn rewards when elected to do so). Without PoW, malicious users could create pseudonymous accounts to undermine the authority or power of a decentralized network or to gain control over it. This is also known as a Sybill attack. However, this approach has downsides, such as the enormous associated energy consumption (de Vries, 2021; O'Dwyer & Malone, 2014) and question marks regarding the security of payments once the block subsidies are phased out (Auer, 2019). PoS is a promising alternative, where Sybil attacks are prevented by, roughly speaking, attributing to each participant in the consensus protocol a weight proportional to their stake as recorded in the ledger itself. PoS also reduced Ethereum energy consumption by more than 99%.[13] Ethereum transitioned to PoS in September 2022 (Ethereum, 2022).

Related risks The DLT technology brings many innovative features, but comes with idiosyncratic risks that can impact the DeFi platforms running atop. Technical issues such as smart contract vulnerabilities can facilitate attacks or exploits, and network congestion can cause delays, disrupting the functioning of DeFi platforms (Chen et al., 2020). High transaction costs can exclude some users from DeFi activity. Another relevant concern is the operational risk related to self-custody. Users may lose their private keys, and with them the access to their funds. Validators can select the transactions recorded on a DLT and order them, potentially affecting the fairness of the system (Stifter et al., 2022). New governance models, by tokenizing voting rights, enable distribution and democratization of decision-making power; however, this poses a centralization threat, as a malicious user could purchase the majority of tokens and manipulate a protocol (Twitter, 2021), and decision-making democratization rarely takes place in reality (Barbereau et al., 2023). Price manipulation is another concern. Oracles are smart contracts that act as a bridge service between a DLT and the external world, allowing to retrieve off-chain data, as well as on-chain data from other DLTs. Oracle manipulation attacks represent a major source of risk for DeFi (Mackinga et al., 2022). Finally, design choices also have implications on user privacy: DLT transactions are publicly auditable, raising privacy-related concerns, especially for account-based DLTs. This highlights the need for privacy-enhancing mechanisms to address concerns surrounding data confidentiality and user anonymity.

[12] A model of the validators' economic incentives underlying the consensus process is discussed in Auer et al. (2022).

[13] See https://ethereum.org/en/energy-consumption/.

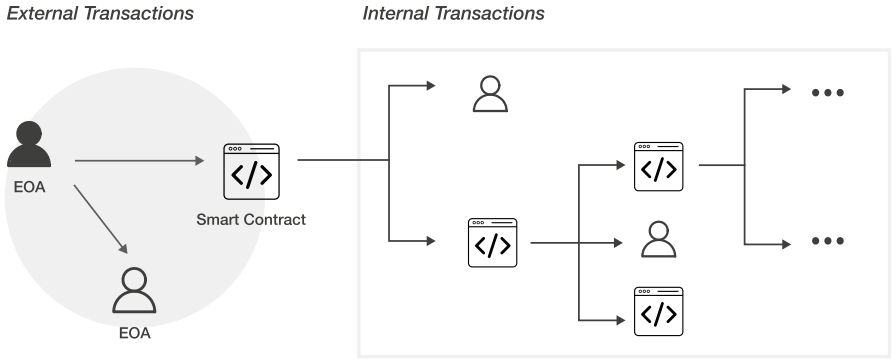

Fig. 2 Account and Transaction Types. An Ethereum transaction always begins with an *external transaction* that can only be initiated by a user account, also known as Externally Owned Account (EOA). It can be directed to another EOA or an account controlled by a smart contract, i.e., a Contract Account (CA). 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, i.e., trigger multiple contracts, which can call other contracts *within the same transaction*

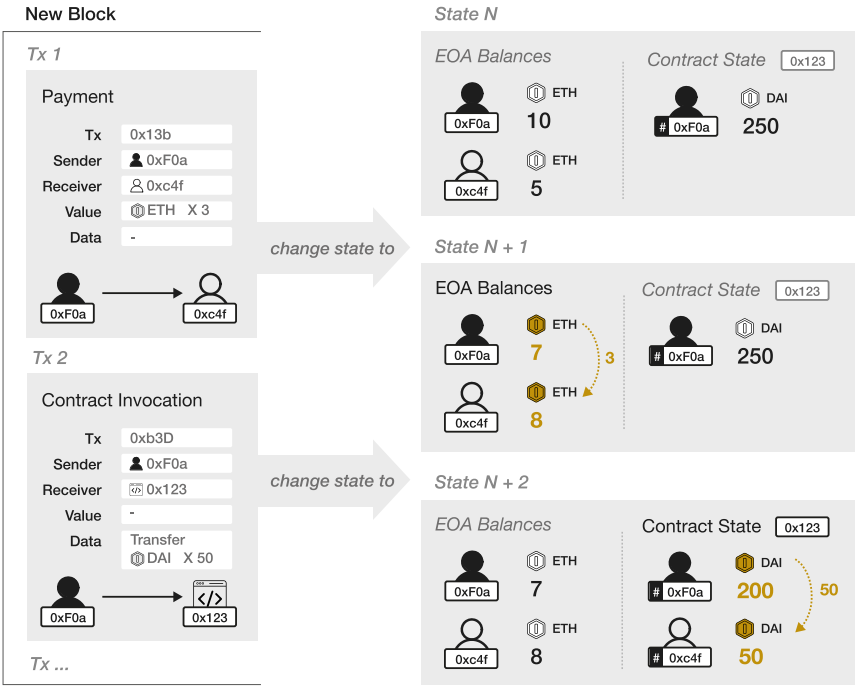

Fig. 3 Transactions in new validated blocks and state changes. Transactions indicate the sender, the receiver, the Ether (ETH) sent, and the data payload. A *Payment* updates the state, e.g., from N to $N + 1$. Ether is transferred from the sender, Alice, to the receiver, Bob. A *Contract invocation* 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

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 (Lausen, 2019). 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, among others, used as a means of exchange, for investment purposes, or to access a good or service.[14]

Figure 4 illustrates a (simplified) taxonomy that introduces the spectrum of cryptoassets.[15] It can be roughly divided based on the conceptual design of their underlying DLT, i.e., the UTXO model or the 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 Litecoin (LTC) and other alt-coins following similar 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, Rosenfeld et al., 2012). 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.[16] The two primary token standards for Ethereum and EVM-based DLTs 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 (Nadini et al., 2021). More recently, NFTs are also issued for 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

[14] European Banking Authority Report with advice for the European Commission on Cryptoassets (European Banking Authority, 2019).

[15] More detailed categorizations can be found in Lausen (2019) and Maia and Santos (2021), that focus on the legal aspects, in Oliveira et al. (2018) that investigates the technical aspect, and Ankenbrand et al. (2020) that provides a more comprehensive approach including multiple aspects.

[16] 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.

could, for instance, be used for loan collateralization or controlling fractional ownership.[17] 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.[18]

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.[19] 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 (Stroponiati et al., 2020). MKR and COMP are governance token examples of the protocols *MakerDAO* and Compound. Governance tokens can be 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 (Barbereau et al., 2022; Jensen et al., 2021).

We note that tokens can have a fixed or a variable supply. In the latter case, tokens can be created and destroyed using specific functions. In jargon, this process is called mint and burn. It respectively indicates the ability to increase the total token supply, or to reduce it by destroying tokens (by sending them to an unspendable address).

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 (Klages-Mundt et al., 2020; Moin et al., 2020) 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 was in the Terra chain before collapse. 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) is backed with cash, commercial paper and corporate bonds (IMF, 2021). USDC and USDT are *centralized* stablecoins: their issuance and redemption on-chain corresponds to fiat transactions, executed off-chain, between the token governance

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

[18] https://centrifuge.io/.

[19] 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.

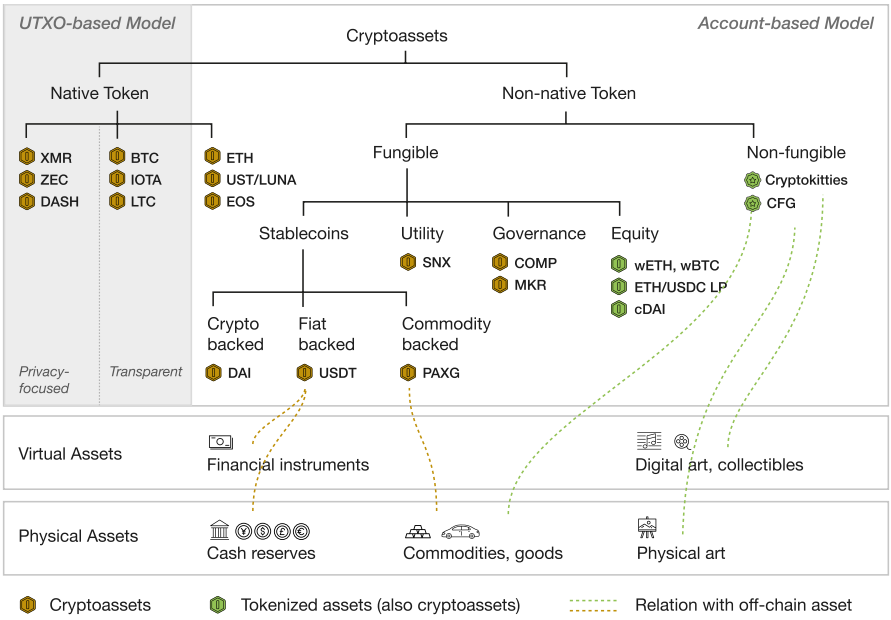

Fig. 4 Cryptoasset taxonomy. DLTs either follow the Bitcoin-like UTXO or the Ethereum-like account model. Both support native tokens (e.g., BTC and ETH). Native tokens can further be divided into privacy-focused (e.g., XMR) or transparent ones (e.g., BTC). Account-model ledgers support the implementation 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

and the investors.[20] Thus, their issuance is not automated and relies on commercial banks. Centralized stablecoins are especially subject to risks: recent investigations on USDT revealed incongruities between official and real reserve assets (Investor Protection Bureau, 2021); USDC lost its peg to the US dollar after the collapse of the Silicon Valley Bank in March 2023. *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 as in the case of Terra tokens UST and LUNA before collapse. In this mechanism, the stablecoin price is related by design to that of another token that absorbs all volatility, and arbitrage mechanisms incentivize users to hold the volatile one (Salehi et al., 2021). The Terra collapse, however, showed that stability pledges of stablecoins are not guaranteed and that they are susceptible to "stablecoin runs" (Klages-Mundt & Minca, 2021).

In general, asset tokenization (Sazandrishvili, 2020) is an essential feature in DeFi. By implementing a dedicated token contract, one can represent any other

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

on- or off-chain asset on a given DLT platform.[21] On Ethereum, for example, one can issue *wrapped tokens*, i.e., 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 (Caldarelli, 2022). It is 1:1 backed with Bitcoin.[22] 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 (Wachter et al., 2021).

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** is a distributed software application that 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. This category also includes protocols that offer insurance services.

Asset management 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 discuss them in Sect. 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

[21] We remark that asset tokenization off-chain is a non-trivial matter, since enforcement of contracts is difficult.

[22] https://wbtc.network/.

main interactions with the economic agents involved.[23] 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* (Warren & Bandeali, 2017) and *EtherDelta* (2022), which exploit the same model deployed in centralized trading platforms, and DEXs with Automated Market Makers, or AMMs (Xu et al., 2022). 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 (Bartoletti et al., 2021; Lehar & Parlour, 2021; Lin, 2019) 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 v3* (Adams et al., 2021b) 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 properties such as the *conservation function* that binds the pooled reserves of the two assets (Angeris & Chitra, 2020). 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.[24]

The spot exchange rate is the token reserve ratio, i.e., y/x. 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 (Angeris et al., 2021). Thus, large enough swaps can cause slippage, i.e., 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 (Wang et al.,

[23] The interactions illustrated in Figs. 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.

[24] See (Adams, 2019; Adams et al., 2021a) The latest version, V3, is based on a similar mechanism but introduces a more complex function (Adams et al., 2021b). Other common types of conservative functions are the constant sum (Krishnamachari et al., 2021) and the geometric mean (Evans, 2021; Evans et al., 2021).

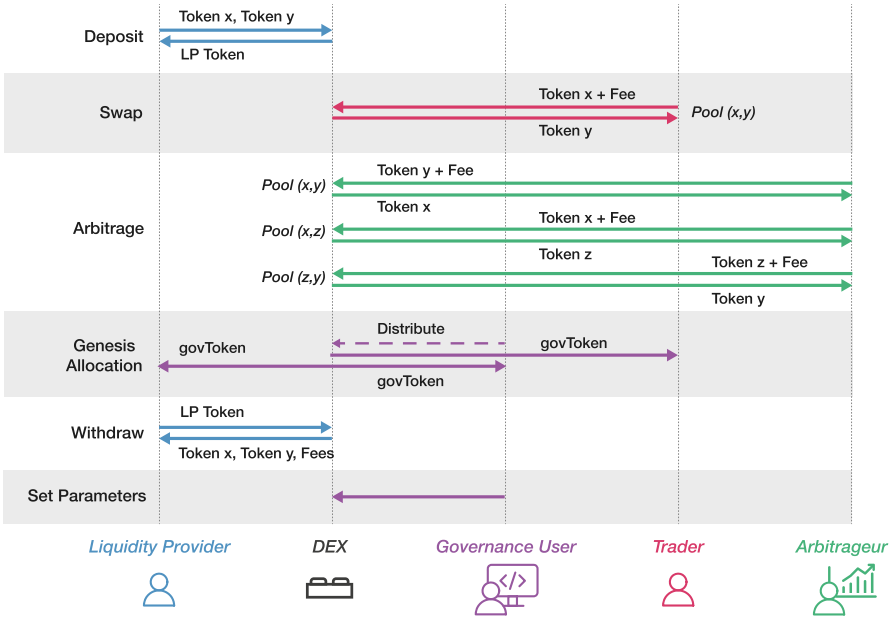

Fig. 5 AMM-based decentralized exchange (DEX). *Traders* are DeFi users who exchange (swap) tokens, while *Liquidity providers (LPs)* deposit and withdraw liquidity in or from pools specific to each trading pair. *Arbitrageurs* rebalance pool compositions when imbalances emerge. Users holding *governance*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

2022) across pools of the same DEX. An alternative strategy is to conduct arbitrage on the same trading pair across different DEXs (Daian et al., 2020), or conducting it on centralized exchanges (Makarov & Schoar, 2020; Saggese et al., 2021).

Liquidity pooling plays an essential role in facilitating token swaps. 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 (Capponi & Jia, 2021). Deposits typically respect the ratio established by the market price[25] 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 (Capponi & Jia, 2021). 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. Notably, the assets ratio in the pool might change in time. Thus, also the prices and the composition of the withdrawn pool share can change. The impermanent loss, or divergence loss, is the opportunity

[25] 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 (Xu et al., 2022).

cost from supplying liquidity instead of simply holding the cryptoassets (Barbon & Ranaldo, 2021).

For completeness, we also mention that in the most recent version of Uniswap (V3) the liquidity provision is more complex, as it allows LPs to 'concentrate' the provided liquidity within an arbitrary price range, and only obtain fees when the price of the token pair is within the specified range. This improves the pool's capital efficiency (Adams et al., 2021b).

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.[26] Thus, incentive mechanisms foster liquidity provision. Part of the fees can be retained in the protocol[27] and managed by the governance, i.e., 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"[28] 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 (Fan et al., 2022). For the period where liquidity mining was active, governance tokens would appear in all user interactions with the protocol in Fig. 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 Examples Other DEXs play a relevant role in DeFi and, thus, deserve special consideration. *SushiSwap* (2022), for instance, is a popular protocol created by forking *UniSwap*; their mechanism design is similar. *Curve* (2022) 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 of liquidity in smaller price ranges. Both exploit more systematically liquidity mining programs. *Balancer* (Martinelli & Mushegian, 2019) and *Bancor* (Hertzog et al., 2017) 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.

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

[27] At the time of writing, *Uniswap* doe not retain fees, unlike other DEXs such as *Sushiswap* (Fritsch et al., 2022).

[28] See https://uniswap.org/blog/uni.

5.2 Lending protocols

Protocols for loanable funds, or PLFs, (Bartoletti et al., 2021), 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 (Aramonte et al., 2022). PLFs operate in a peer-to-pool fashion: borrowers interact with smart contracts that *pool the liquidity*, i.e., resources supplied by cryptoasset lenders. An essential difference to loans issued by traditional financial institutions is that interest rates are set automatically (Xu & Vadgama, 2022), 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 (Huber & Treytl, 2022).[29]

Typically, borrowing is allowed only after collateral provision as a protection against the counterparty risk of default. PLFs often require such positions to be overcollateralized due to cryptoassets volatility and to counterparty anonymity (Aramonte et al., 2022). However, this is not always the case, and some protocols like Clearpool (2022) allow to open unsecured positions, by enabling users to lend directly to whitelisted institutions. Flash loans are another uncollateralized lending mechanism, enabled by DeFi, that eliminates default risk: loans are either atomically executed and repaid within one individual transaction or reverted (Qin et al., 2021).[30]

Financial Services Figure 6 shows how the economic agents interact with financial services offered by lending protocols such as *Compound* (Leshner & Hayes, 2019). 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 (Saengchote, 2022). 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, i.e., they rise sharply after a specific borrowing utilization ratio against the deposited funds, while other PLFs follow linear and non-linear models (Gudgeon et al., 2020).

The *collateralization* of debt positions is a core financial function PLF contracts build upon. In *Compound*, collateral is provided by interacting with the same contract functions that serve to supply liquidity[31]; 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.

[29] Regarding interest rates, we mention IPOR, a project that aims to provide benchmark rates for DeFi.

[30] While almost risk-free for the lender, they may facilitate attacks to DeFi protocols. For instance, they can be used for market manipulation, leading to artificially inflating or deflating prices. They have also been used to exploit DeFi smart contract vulnerabilities and drain funds from them. See e.g. https://hacken.io/discover/crypto-hacks/.

[31] See https://bit.ly/41akDfk.

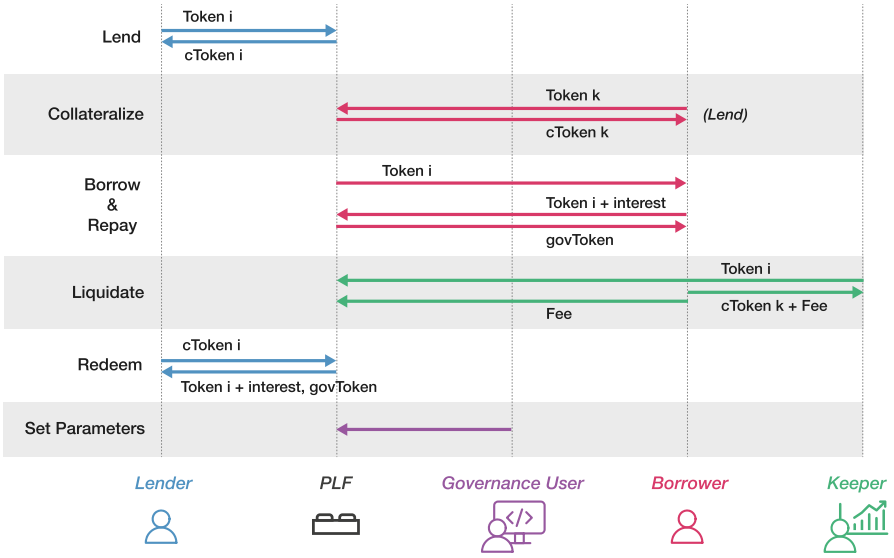

Fig. 6 Lending protocol. *Borrowers* take out loans on funds supplied by *Lenders*, and their default risk is hedged by overcollateralizing their positions. *Keepers* close insufficiently collateralized positions for a fee. *Governance* members earn fees from protocol usage

Price fluctuations can lead to insufficiently collateralized positions: if the borrower does not provide additional capital, the loan may be liquidated (Perez et al., 2021). *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 (Kao et al., 2020). At the new market prices, either the remaining borrower's collateral is sufficient to back the fraction of loaned cryptoassets that were not liquidated,[32] or it will be subject to subsequent liquidations. Part of the fees can be retained within the protocol.[33] 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 (Qin et al., 2021). 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 characteristics.

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

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

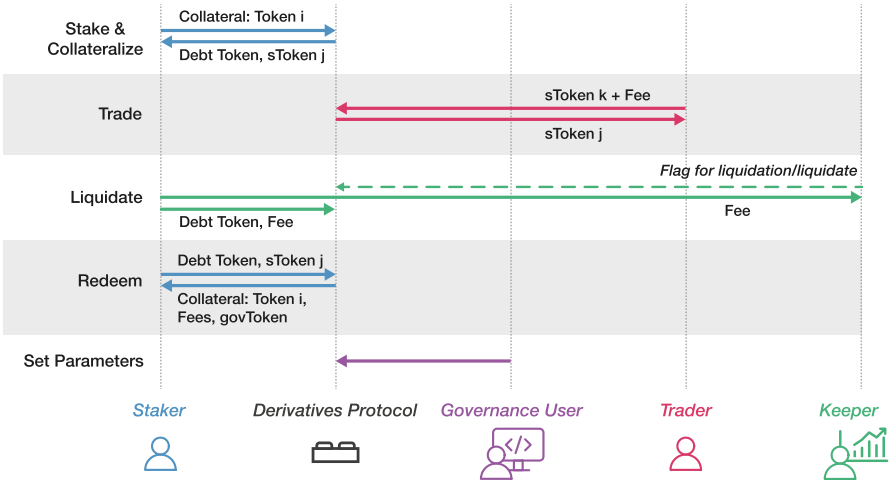

Fig. 7 Derivatives protocols. *Stakers* supply capital in a pooling contract for a reward, *Traders* swap derivative products like in DEXs. Similarly to PLFs, *Keepers* auction insufficiently collateralized positions. *Governance users* have voting rights and decision-making power

Other Examples *Aave* (2020) is among the largest PLFs by TVL. It provides similar financial services to *Compound*, and users can choose between stable and variable interest rates. *MakerDAO* (2020) is another lending protocol that allows locking capital to mint DAI. Other relevant protocols categorized as PLFs are *Alpha Homora* (2021) and *Liquity* (Lauko & Pardoe, 2021).

5.3 Derivatives protocols

We now consider the protocols that issue and facilitate the trading of financial derivative contracts in a decentralized context.[34] 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 (Kumar, 2022). The spectrum of derivatives protocols ranges from call and put options over futures, forward contracts, and perpetual swaps (Soska et al., 2021). Synthetic assets enable exposure to an asset without actual ownership. To trace the underlying assets' price, these DeFi protocols exploit *Oracles*. 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 to protect against risks.

[34] In this subsection we focus on the design of protocols that enable issuing derivatives. However, we remark that this category also includes protocol that provide insurance services, such as *Nexus* (Karp & Melbardis, 2022).

DeFi options vaults (DOVs) are derivatives protocols that gained relevance after mid 2021. These protocols invest the investors' assets staked into vaults, i.e., smart contracts that deploy the assets into options strategies, for instance by automating covered calls or put strategies (Ribbon Finance, 2022). They aim to generate sustainable, risk-adjusted yield, based on the payment of option premiums that exploit the high volatility of the market, rather than on token rewards alone.

Financial Services Figure 7 illustrates the interactions between a derivatives protocol and the economic agents involved, using as a reference the protocol *Synthetix* (2022). 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.[35] 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 (Synthetix, 2022).

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.[36]

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.[37]

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

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

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

Other Examples Other relevant protocols are *dYdX* (Juliano, 2018) and *Nexus* (Karp & Melbardis, 2022). 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* (2021) offers tools to tokenize and hence hedge risk, while *Hegic* (2020) offers many different derivative contract options. Examples of DeFi option vaults are Ribbon Finance (2022), Thetanuts Finance (2023), and StakeDAO (2022).

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[38] 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 (Xu et al., 2022; Xu & Xu, 2022). 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 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 (Salehi et al., 2021). DEXs exploit bonding curves and conservation pricing functions to price assets relative to one another, and Oracles are utilized to incorporate external sources of information into the protocol.

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

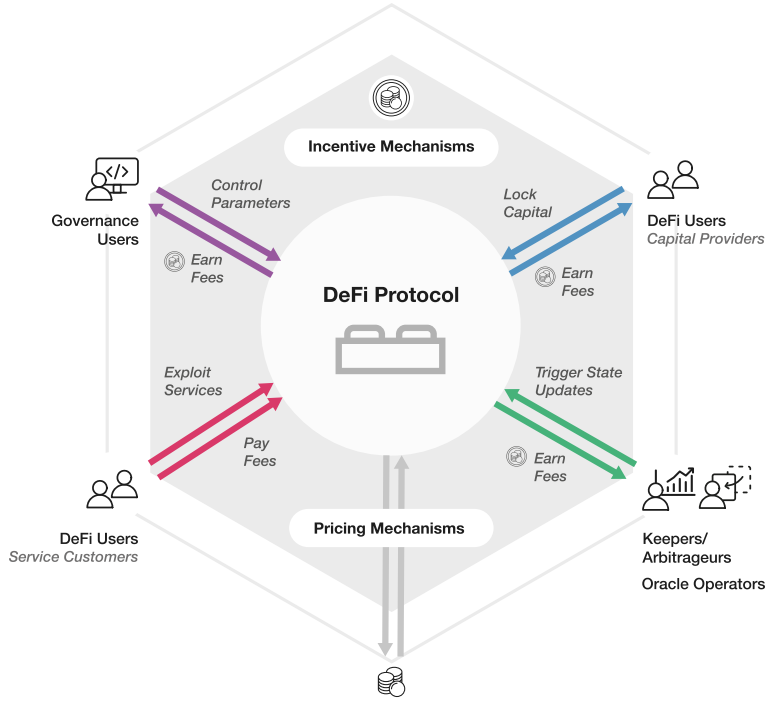

Fig. 8 DeFi peer-to-pool model. Generalization of the interactions between economic actors and the DeFi protocols. The DeFi users that exploit the protocols by demanding liquidity pay a fee for accessing their services, while those that provide liquidity passively interact with them and earn an income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

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 (Engel & Herlihy, 2021; Tolmach et al., 2021). Since composability has become a central aspect of current DeFi developments (Wachter et al., 2021), we now focus on interactions at the smart contract level.

6.1 Conceptualization

To illustrate the concept of a DeFi composition, we recall that smart contracts can interact with other smart contracts within one individual transaction and refer to Fig. 9. It shows the execution of two transactions at the smart contract level. Both use the *same* financial service, i.e., a swap of two tokens (wETH and USDT) executed by the *UniSwap* DeFi protocol. The one on top is initiated by an EOA interacting with the "Router" smart contract of the *1inch* protocol, while the one on the

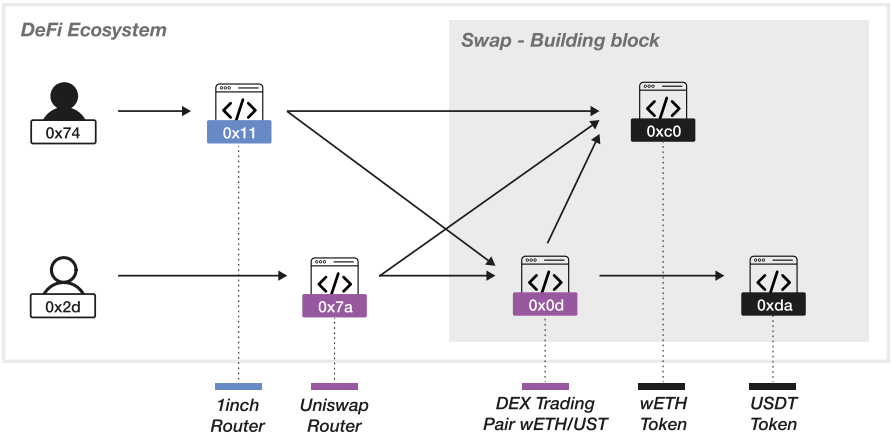

Fig. 9 DeFi composition example. Illustration of two distinct transactions at the smart contract level. The colored rectangles indicate protocol-specific smart contracts, and the colors are used to distinguish those associated with different DeFi protocols (blue for *1inch* and pink for *UniSwap*). To 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

bottom is directed to *UniSwap*'s "Router" contract.[39] The purpose of the *1inch* protocol is to compare prices across several DEXs and to redirect 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, i.e., 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 EOAs. Given this conceptualization, and following Kitzler et al. (2022b), we define the notion of a "DeFi Composition" as follows:

Definition 3 A **DeFi composition** provides novel financial services by utilizing a combination of smart contracts associated with multiple protocols within a single transaction.

We envision two key features that DeFi offers through compositions: the first one, as discussed above, entails offering new services that could not be offered by individual DeFi protocols alone. The former is an example of composable liquidity, whereby any exchange service can exploit the liquidity and exchange rates of any other exchange contract (Harvey, 2021). The second is that, in principle,

[39] The router contract indicates, in this context, the contract that enables token swaps and calculates prices. It also enables users to add and remove liquidity.

composability allows to combine financial services that are harder to integrate in traditional finance. For instance, it might facilitate the tokenization and fractional ownership of assets that can be traditionally illiquid, their subsequent trade on a DEXs, or their use as collateral to borrow other assets which in turn can be reinvested — all within one transaction. This might reduce inefficiencies and costs for moving funds from one institutions to another while making the entire process faster. The potential advantages (and risks) of composability in DeFi yet have to be fully explored.

6.2 Aggregators

At the time of writing, Aggregators is the most relevant DeFi protocol category. 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, i.e., services that implement strategies to maximize the users return across multiple DeFi protocols.

Yield Aggregators (Xu & Feng, 2022) 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 (Popescu, 2020). The optimization strategies and the underlying assets differ across protocols, but their mechanism is similar: users lock capital in a contract that allocates it programmatically to a set of other DeFi financial instruments, according to user preferences, such as risk profiles, and governance parameters (Schär, 2021). 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* (2022). 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 (Schär, 2021).

Once a strategy is devised, a Vault contract is created to collect investors' funds. In *Idle*'s Best Yield strategy,[40] the Vault collects single cryptoassets supplied by individual *Investors*, which in turn receive strategy tokens, i.e., 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,

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

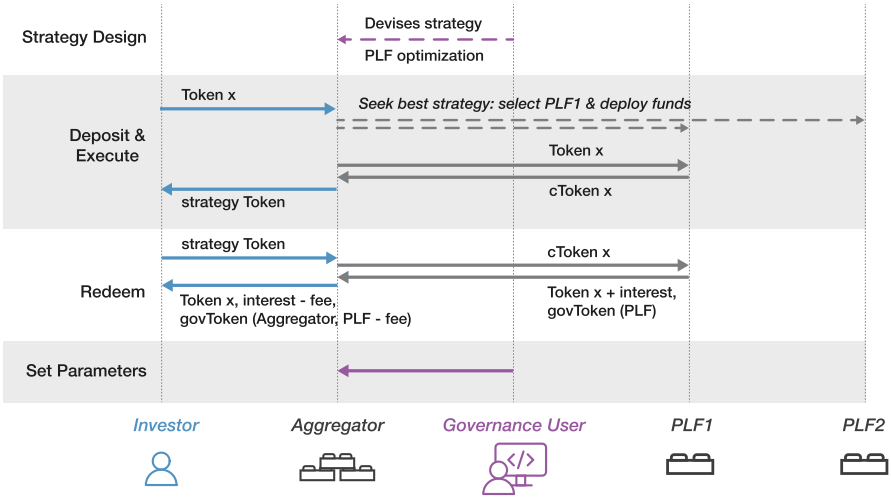

Fig. 10 Yield aggregators. The *Governance* proposes yield farming investment strategies and has voting power. *Investors* lock their capital to a "Vault" smart contract. The Aggregator in turn interacts with other DeFi protocols, in this example PLF_1 and PLF_2. Rewards are then distributed to Investors

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* (Cousaert et al., 2022).

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 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.[41] 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* (2022) base their strategies on investing in LP tokens associated with liquidity pools with the highest returns on investment. *Harvest Finance* (2022) offers the possibility to choose between both strategies. Others, like *Yearn Finance* (2020), 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* (Santoro, 2021) or wBTC such as *Badger* (2022).

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

6.3 Investigating DeFi compositions

The example illustrated in Fig. 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 Fig. 10 describes how Aggregators exploit financial services provided by other protocols. However, previous work (Kitzler et al., 2022c) 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 Sect. 1, there is a clear need to investigate and better understand such compositions. To do so, and following Kitzler et al. (2022b), we identified two possible directions that we describe below.

Building Block Extraction Identifying 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. For instance, the "Swap" in Fig. 9 is a building block: it always has the same structure and financial function, independently of the tokens involved in the swap. Noteworthy, building blocks can also contain other building blocks in a nested structure. In Kitzler et al. (2022c), authors propose 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 DeFi protocol-specific smart contracts and construct a network in which nodes represent smart contracts and edges represent the transactions involving specific source and target contracts. 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,[42] 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 (as in the example shown in Fig. 9). Thus, edges indicate the existence of DeFi compositions. The network is highly connected: DeFi protocols heavily rely on each other.

[42] *0x*, *1inch*, *Balancer*, *Curvefinance*, *SushiSwap*, *UniSwap*, *Aave*, *Compound*, *Instadapp*, *MakerDAO*, *Barnbridge*, *dYdX*, *Futureswap*, *Hegic*, *Nexus*, *Syntetix*, *Badger*, *Convex*, *Fei*, *Harvestfinance*, *RenVM*, *Vesper*, *Yearn*.

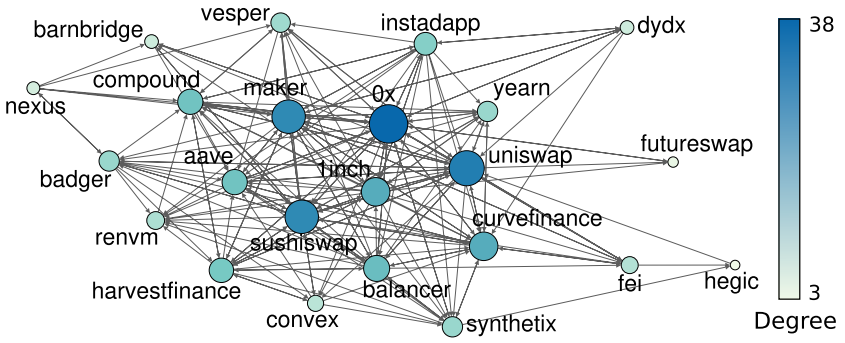

Fig. 11 The DeFi protocol network. The plot represents the network of DeFi protocols (nodes) and their interactions (edges). The network is constructed from a dataset of external transactions directed to a set of smart contracts manually associated with 23 DeFi protocols and the subsequent internal transactions. 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

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 depeg from USD, and the price of its native tokens LUNA and UST fell close to zero in a few hours (Briola et al., 2023). 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 Kitzler et al. (2022c). 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 Fig. 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

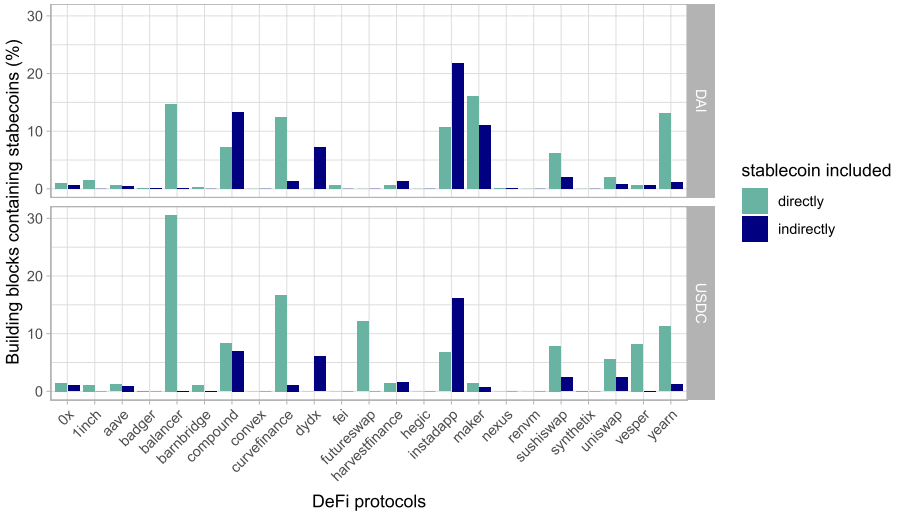

Fig. 12 Protocol exposure to stablecoin runs. For each of the 23 DeFi protocols in our dataset, we measure the fraction of building blocks that are directly or indirectly dependent on DAI (top panel) and on USDC (bottom panel). While most protocols do not rely heavily on stablecoins, a few of them have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

Yearn, *Curvefinance*, and *Compound*. In summary, these results illustrate that 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.

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 Sect. 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 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.[43] 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[44] 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,[45] and we note that many of the protocols described in Sect. 5 are now deploying their smart contracts in multiple DLTs (thus, we call them *multichain* protocols).

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 (Robinson, 2021). The challenge lies in finding mechanisms that allow a source ledger to change the state of a target ledger (Belchior et al., 2021).

Atomic swaps represent a way for two counterparts to coordinate on the exchange of native tokens, by executing transactions on multiple DLTs (Herlihy, 2018; Tsabary et al., 2021; Xu et al., 2021). *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 a 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* (Singh et al., 2020) 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). Similarly to sidechains, "Layer 2" protocols offer scaling solutions (Gudgeon et al., 2020; Sguanci et al., 2021). However, they entail the execution of a batch of transactions off-chain so that only the final state is recorded on-chain, and do not modify the DLT trust assumptions, nor the consensus mechanism.

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* (Wood, 2016), for instance, the Relay Chain plays a central role, and additional blockchains that interoperate by default, called parachains, can be created. *Cosmos* (Kwon & Buchman, 2019) implements a similar design. It targets generic blockchain interoperability and is also based on a structure with a main blockchain,

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

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

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

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. 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). One relevant future research direction entails understanding how this aspect will affect the DeFi ecosystem. For instance, it would be interesting to understand if having multiple DeFi protocols built on different DLTs will increase competition, or if it will have negative impact such as fragmented liquidity. Analyzing and measuring the composition of cryptoasset flows across DLTs is an additional promising research direction.

Transaction Reordering and Mining Miners can choose which transactions to include and how to order them when new blocks are appended to the blockchain. This practice, known as transaction reordering, may affect the outcome and profitability of trading activity involving other DeFi actors (Stifter et al., 2022). The resulting profit is called maximal extractable value (MEV). For instance, if a transaction that closes an arbitrage opportunity is broadcast to the network, miners could execute an identical transaction, and order in the block so that it executes before the original transaction (i.e., a front-running attack). This has implications both on miners' incentives and on the DeFi users trading activity. From an economic perspective, these aspects can be approached using game-theoretic analysis and related methodologies. In Canidio and Danos (2022), for instance, the authors exploit game theory to distinguish legitimate competition from attacks that aim at maximize MEV. Previous research (Qin et al., 2022) 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 liquidations and arbitrage actions are relevant sources of MEV, extracted through techniques based on transaction ordering such as front-running attacks. Furthermore, centralized servers called relayers put miners in direct contact with third parties that look for MEV opportunities systematically. The latter pay miners to order transactions as they request. The model introduced in Capponi et al. (2022) investigates the economic incentives behind the adoption of such services. Further research in this direction is needed, to better understand how to prevent 'unfair' activity such as transaction reordering, and to what extent DeFi composability exacaberates transaction reordering-related issues.

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 (Canidio, 2022), or aim at investigating what cryptoassets and how DeFi could facilitate illicit activities (Paquet-Clouston et al., 2019).

7.3 DeFi protocols

At the time of writing, leading 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 Sect. 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 (Capponi & Jia, 2021). 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 (Zargham et al., 2020). 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 (Fukasawa et al., 2023). 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 Canidio (2022).

Another relevant aspect to investigate in greater detail regards how the governance of DeFi protocols is managed and how this affects centralization (Makridis et al., 2021). 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, 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 cryptoassets.

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 systemic risk assessment. Previous studies have investigated, for instance, under what market conditions DeFi protocols that exploit overcollateralization might suffer from drying-up liquidity issues and become insolvent (Gudgeon et al., 2020). Also, repeatedly tokenized assets can create dependencies across DeFi actors (Wachter et al., 2021) and raise stability concerns. Future research should focus on understanding systemic risk more profoundly, for instance by analyzing token flows (Kitzler et al., 2022a) and protocol dependencies, both within the crypto-ecosystem and by considering the potential spillovers from and to the traditional financial system (Diem et al., 2020; Lindner et al., 2019). 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 can be assembled into complex financial constructs through compositions. We also pointed out possible investigation and measurement methods 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.

Author contributions PS wrote the manuscript with the support of BH and RA; SK and FV supported PS in conducting the analyses in Section 6 and preparing the Figures 5–7, 10, 12. All authors contributed to the preparation of Figure 1 and all authors reviewed the manuscript.

Data availability Data are available and can be requested to the corresponding author upon request.

Declarations

Conflict of interest The authors declare no competing interests.

References

Aave. (2020). *Protocol whitepaper*. Technical report, Available at https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf

Adams, H. (2019). *Uniswap v1 whitepaper*. Technical report. Available at https://hackmd.io/@HaydenAdams/HJ9jLsfTz.

Adams, H.. et al. (2021a). *Uniswap v2 core*. Technical report. Available at https://uniswap.org/whitepaper.pdf.

Adams, Z., Salem, M., Keefer, R., & Robinson, D. (2021b). *Uniswap v3 core*. Technical report. Available at https://uniswap.org/whitepaper-v3.pdf

Alpha Venture DAO. (2021). *Alpha homora v2*. Technical report. Available at https://github.com/AlphaFinanceLab/alpha-homora-v2-contract

Angeris, G., & Chitra, T. (2020). Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, AFT '20 (pp. 80–91). Association for Computing Machinery. https://doi.org/10.1145/3419614.3423251

Angeris, G., Kao, H. T., Chiang, R., Noyes, C., & Chitra, T. (2021). An analysis of uniswap markets. *Cryptoeconomic Systems*. https://doi.org/10.21428/58320208.c9738e64

Ankenbrand, T., Bieri, D., Cortivo, R., Hoehener, J., & Hardjono, T. (2020). Proposal for a comprehensive (crypto) asset taxonomy. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 16–26). IEEE. https://doi.org/10.1109/CVCBT50464.2020.00006

Aquilina, M., Frost, J., & Schrimpf, A. (2022). Decentralised Finance (DeFi): A Functional Approach. *Available at SSRN:* https://doi.org/10.2139/ssrn.4325095

Aramonte, S., Doerr, S., Huang, W., Schrimpf, A., et al. (2022). *Defi lending: intermediation without information?* Bank for International Settlements. Technical report.

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*, page 21.

Atzei, N., Bartoletti, M. C., Tiziana, L. S., & Zunino, R. (2018). Sok: Unraveling bitcoin smart contracts. In *International Conference on Principles of Security and Trust* (pp. 217–242). Springer. https://ia.cr/2018/192

Auer, R. (2019). Beyond the doomsday economics of "proof-of-work" in cryptocurrencies. *Bank for International Settlements Working Papers 765*.

Auer, R., Farag, M., Lewrick, U., Orazem, L., & Zoss, M. (2022). Banking in the shadow of bitcoin? the institutional adoption of cryptocurrencies. *Bank for International Settlements Working Papers 1013*.

Auer, R., Frost, J., Pastor, J., María, V., et al. (2022). Miners as intermediaries: Extractable value and market manipulation in crypto and DeFi. *Bank for International Settlements*. Technical report.

Auer, R., Monnet, C., & Shin, H.S. (2022). Distributed ledgers and the governance of money. *Bank for International Settlements Working Papers 924*.

Auer, R, Frost, J, Vidal, P, & Jose, M. (2022). Miners as intermediaries: Extractable value and market manipulation in crypto and DeFi. *Bank for International Settlements Bulletins, 58*.

Badger. (2022). *Gitbook*. Technical report. Available at https://docs.badger.com/

Barbereau, T., Smethurst, R., Papageorgiou, O., Rieger, A., & Fridgen, G. (2022). DeFi, not so decentralized: The measured distribution of voting rights. In *Proceedings of the 55th Hawaii International Conference on System Sciences*. http://hdl.handle.net/10125/80074

Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society, 73*, 102251. https://doi.org/10.1016/j.techsoc.2023.102251

Barbon, A., & Ranaldo, A. (2021). On the quality of cryptocurrency markets: Centralized versus decentralized exchanges. *arXiv preprint*arXiv:2112.07386.

Barnbridge. (2021). *Barnbridge—a fluctuations derivatives protocol for hedging yield sensitivity and market price*. Technical report. Available at https://github.com/BarnBridge/BarnBridge-Whitepaper.

Bartoletti, M., Chiang, J. H., & Lafuente, A. L. (2021). Sok: Lending pools in decentralized finance. In *International Conference on Financial Cryptography and Data Security, FC 2021 International Workshops* (pp. 553–578). Springer. https://doi.org/10.1007/978-3-662-63958-0_40

Bartoletti, M., Chiang, J. H., & Lluch-Lafuente, A. (2021). A theory of automated market makers in DeFi. In *International Conference on Coordination Languages and Models* (pp. 168–187). Springer. https://doi.org/10.46298/lmcs-18(4:12)2022

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR), 54*(8), 1–41. https://doi.org/10.1145/3471140

BIS. (2003). *A glossary of terms used in payments and settlement systems*. Technical report, Bank for International Settlements.

BIS. (2022a). *Annual economic report. chapter 3: The future monetary system*. Technical report, Bank for International Settlements.

BIS. (2022b). *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.

Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2023). Anatomy of a stablecoin' failure: The terra-luna case. *Finance Research Letters, 51*, 103358. https://doi.org/10.1016/j.frl.2022.103358

Caldarelli, G. (2022). Wrapping trust for interoperability: A preliminary study of wrapped tokens. *Information, 13*(1), 6. https://doi.org/10.3390/info13010006

Canidio, A. (2022). *Auctions with tokens*. Available at: https://www.dropbox.com/s/dksejx5h7sye2ms/Canidio-Auctions-with-tokens.pdf?dl=0.

Canidio, A., & Danos, V. (2022). *Commitment against front running attacks*. Available at: https://www.dropbox.com/s/pmketrifnnfv2nu/Canidio-Danos-front-running.pdf?dl=0.

Capponi, A., & Jia, R. (2021). The adoption of blockchain-based decentralized exchanges. *arXiv preprint*arXiv:2103.08842.

Capponi, A., Jia, R., & Wang, Y. (2022). The evolution of blockchain: From lit to dark. *arXiv preprint*arXiv:2202.05779.

Carter, N., & Jeng, L. (2021). Defi protocol risks: The paradox of defi, Chapter of "Regtech, Suptech and Beyond: Innovation and Technology in Financial Services", RiskBooks.

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS), 20*(4), 398–461. https://doi.org/10.1145/571637.571640

Chen, T., Li, Z., Zhang, Y., Luo, X., Chen, A., Yang, K., Hu, B., Zhu, T., Deng, S., Hu, T. (2019). Dataether: Data exploration framework for ethereum. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1369–1380). IEEE. https://doi.org/10.1109/ICDCS.2019.00137

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computer of Survey, 53*(3), 1–43. https://doi.org/10.1145/3391195

Clearpool. (2022). *Protocol whitepaper*. Technical report. Available at https://docs.clearpool.finance/clearpool/resources/whitepaper.

Cousaert, S., Xu, J., & Matsui, T. (2022). Sok: Yield aggregators in DeFi. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–14). IEEE. https://doi.org/10.1109/ICBC54727.2022.9805523

Curve Protocol. (2022). *Curve documentation*. Technical report. Available at https://curve.readthedocs.io/_/downloads/en/latest/pdf/.

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

de Vries, Alex. (2021). Bitcoin boom: What rising prices mean for the network's energy consumption. *Joule, 5*(3), 509–513. https://doi.org/10.1016/j.joule.2021.02.006

DeFiLama. (2022). Available at: https://defillama.com/.

Diem, C., Pichler, A., & Thurner, S. (2020). What is the minimal systemic risk in financial exposure networks? *Journal of Economic Dynamics and Control, 116*, 103900. https://doi.org/10.1016/j.jedc.2020.103900

Donmez, A., & Karaivanov, A. (2022). Transaction fee economics in the ethereum blockchain. *Economic Inquiry, 60*(1), 265–292. https://doi.org/10.1111/ecin.13025

El Ioini, N., & Pahl, C. (2018). A review of distributed ledger technologies. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"* (pp. 277–288). Springer. https://doi.org/10.1007/978-3-030-02671-4_16

Engel, D., & Herlihy, M. (2021). Composing networks of automated market makers. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* (pp. 15–28). https://doi.org/10.1145/3479722.3480987

Etherdelta. (2022). *Etherdelta protocol*. Available at https://etherdelta.com/.

Ethereum. (2022). *The ethereum merge*. Available at https://ethmerge.com/.

European Banking Authority. (2019). *Eba reports on crypto-assets*. Available at https://www.eba.europa.eu/eba-reports-on-crypto-assets.

Evans, A. (2021). Liquidity provider returns in geometric mean markets. *Cryptoeconomic Systems, 1*, (2). https://doi.org/10.21428/58320208.56ddae1b

Evans, A., Angeris, G., & Chitra, T. (2021). Optimal fees for geometric mean market makers. In *International Conference on Financial Cryptography and Data Security* (pp. 65–79). Springer. https://doi.org/10.1007/978-3-662-63958-0_6

Fan, S., Min, T., Wu, X., & Wei, C. (2022). Towards understanding governance tokens in liquidity mining: A case study of decentralized exchanges. *World Wide Web*. https://doi.org/10.1007/s11280-022-01077-4

Fritsch, R., Käser, S., & Wattenhofer, R. (2022). The economics of automated market makers. *arXiv preprint*arXiv:2206.04634.

FSB. (2022). *Assessment of risks to financial stability from crypto-assets*. Technical report, Financial Stability Board.

Fukasawa, M., Maire, B., & Wunsch, M. (2023). Weighted variance swaps hedge against impermanent loss. *Quantitative Finance*, *23*, 901–911. https://doi.org/10.1080/14697688.2023.2202708

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). Sok: Layer-two blockchain protocols. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (pp. 201–226). Springer. https://doi.org/10.1007/978-3-030-51280-4_12

Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 1–15). IEEE. https://doi.org/10.1109/CVCBT50464.2020.00005

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

Harvest Finance. (2022). *Harvest finance protocol*. Technical report. Available at https://harvest-finance.gitbook.io/harvest-finance/.

Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the future of finance*. John Wiley & Sons.

Herlihy, M. (2018). Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254.

Hertzog, E., Benartzi, G., & Benartzi, G. (2017) *Bancor protocol*. Technical report. Available at https://cryptopapers.info/assets/pdf/bancor.pdf

Huber, M., & Treytl, V. (2022). Risks in DeFi-lending protocols-an exploratory categorization and analysis of interest rate differences. In *International Conference on Database and Expert Systems Applications* (pp. 258–269). Springer. https://doi.org/10.1007/978-3-031-14343-4_24

Idle Finance. (2022). *Documentation*. Tech. rep., See https://docs.idle.finance/.

IMF. (2021). *Global Financial Stability Report: October 2021*. Technical report, International Monetary Fund.

Investor Protection Bureau. (2021). *Attorney general james ends virtual currency trading platform bitfinex's illegal activities in New York*. Available at https://on.ny.gov/3izikSX.

Itay, T., Yechieli, M., Manuskin, A., & Eyal, I. (2021). Mad-htlc: Because htlc is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 1230–1248). IEEE. https://doi.org/10.1109/SP40001.2021.00080

Jensen, J.R., von Wachter, V., & Ross, O. (2021). How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions. *arXiv preprint* arXiv:2102.10096

Juliano, A. (2018). *dYdX: A standard for decentralized margin trading and derivatives*. Technical report. Available at https://whitepaper.dydx.exchange/

Kao, H. T., Chitra, T., Chiang, R., & Morrow, J. (2020). An analysis of the market risk to participants in the compound protocol. In *Third International Symposium on Foundations and Applications of Blockchains*.

Karp, H., & Melbardis, R. (2022). *Nexus mutual—a peer-to-peer discretionary mutual on the ethereum blockchain*. Technical report. Available at https://nexusmutual.io/assets/docs/nmx_white_paper v2_3.pdf

Kitzler, S., Diem, C., Saggese, P., Haslhofer, B., & Thurner, S. (2022a). Systemic risk in decentralized finance (DeFi)—an investigation of smart contract interdependencies. In *11th International Conference on Complex Networks and Their Applications*. https://doi.org/10.5281/zenodo.7593062

Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2022b). A systematic investigation of DeFi compositions in ethereum. In *The 2nd Workshop on DeFi, International Conference on Financial Cryptography and Data Security*. https://doi.org/10.1007/978-3-031-32415-4_18

Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2022c). Disentangling decentralized finance (defi) compositions. *ACM Transactions on the Web, 17*(2), 1–26. https://doi.org/10.1145/3532857

Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J. Y., & Minca, A. (2020). Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (pp. 59–79). https://doi.org/10.1145/3419614.3423261

Klages-Mundt, A., & Minca, A. (2021). (In)Stability for the blockchain: Deleveraging spirals and stablecoin attacks. *Cryptoeconomic Systems, 1*(2). https://doi.org/10.21428/58320208.e46b7b81

Krishnamachari, B., Feng, Q., & Grippo, E. (2021). Dynamic curves for decentralized autonomous cryptocurrency exchanges. *arXiv preprint*arXiv:2101.02778.

Kumar, S. (2022). Central clearing of crypto-derivatives in a decentralized finance (defi) framework: An exploratory review. *International Journal of the Economics of Business, 7*(1), 128. https://doi.org/10.5281/zenodo.6596485

Kwon, J., & Buchman, E. (2019). *Cosmos whitepaper*. Ledgers: A Netw Distrib.

Lauko, R., & Pardoe, R. (2021). *Liquity: Decentralized borrowing protocol*. Technical report. Available at https://docsend.com/view/bwiczmy.

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

Lehar, A., & Parlour, C. A. (2021). *Decentralized exchanges*. Available at SSRN 3905316.

Leshner, R., & Hayes, G. (2019). *Compound: The money market protocol*. Technical report. Available at https://bit.ly/3ioWOjW.

Lin, L. X. (2019). Deconstructing decentralized exchanges. *Stanford Journal of Blockchain Law and Policy, 2*, 58.

Lindner, P., Loeffler, A., Segalla, E., Valitova, G., & Vogel, U. (2019). International monetary policy spillovers through the bank funding channel. *Journal of International Money and Finance, 90*, 161–174. https://doi.org/10.1016/j.jimonfin.2018.08.012

Mackinga, T., Nadahalli, T., & Wattenhofer, R. (2022). Twap oracle attacks: Easier done than said? In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICBC54727.2022.9805499

Maia, G. C., & Vieira dos Santos, J. (2021). *Mica and DeFi ('proposal for a regulation on market in crypto-assets' and 'decentralised finance')*. Available at SSRN 3875355.

Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics, 135*(2), 293–319. https://doi.org/10.1016/j.jfineco.2019.07.001

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

Makridis, C., Froewis, M., Sridhar, K., & Böhme, R. (2021). The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Journal of Corporate Finance*, *79*, 102358. https://doi.org/10.1016/j.jcorpfin.2023.102358

Martinelli, F., & Mushegian, N. (2019). *Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor.* Technical report. Available at https://balancer.fi/whitepaper.pdf

Moin, A., Sekniqi, K., & Sirer, E. G. (2020). Sok: A classification framework for stablecoin designs. In *International Conference on Financial Cryptography and Data Security* (pp. 174–197). Springer. https://doi.org/10.1007/978-3-030-51280-4_11

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the nft revolution: Market trends, trade networks, and visual features. *Scientific Reports, 11*(1), 1–11. https://doi.org/10.1038/s41598-021-00053-8

Nelson, D., & Wang, T. (2022). 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/

Nuzzi, L., Calvez, A.L., & Waters, K. (2021). Understanding total value locked (tvl). Available at: https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-0c0

O'Dwyer, K. J., & Malone, D. (2014). 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 2014CIICT 2014)* (pp. 280–285). https://doi.org/10.1049/cp.2014.0699

Oliveira, L., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To token or not to token: Tools for understanding blockchain tokens. In *International Conference of Information Systems (ICIS 2018)*, San Francisco, USA, December ICIS. https://doi.org/10.5167/uzh-157908

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity, 5*(1), tyz003. https://doi.org/10.1093/cybsec/tyz003

Perez, D., Werner, S. M., Xu, J., & Livshits, B. (2021). Liquidations: Defi on a knife-edge. In *International Conference on Financial Cryptography and Data Security* (pp. 457–476). Springer. https://doi.org/10.1007/978-3-662-64331-0_24

Pickle Finance. (2022). *Documentation.* Tech. rep., See https://docs.pickle.finance/

Popescu, A. D. (2020). Transitions and concepts within decentralized finance (DeFi) space. *Research Terminals in the Social Sciences*.

Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An empirical study of DeFi liquidations: Incentives, risks, and instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*. https://doi.org/10.1145/3487552.3487811

Qin, K., Zhou, L., & Gervais, A. (2022). Quantifying blockchain extractable value: How dark is the forest? In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 198–214). IEEE. https://doi.org/10.1109/SP46214.2022.9833734

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the DeFi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security* (pp. 3–32). Springer. https://doi.org/10.1007/978-3-662-64322-8_1

Rai, R. (2022). The death spiral: How terra'salgorithmic stablecoin came crashing down. Available at: https://www.forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down/?sh=41275c6a71a2.

Ribbon Finance. (2022). *Documentation*. Available at https://docs.ribbon.finance/.

Robinson, P. (2021). Survey of crosschain communications protocols. *Computer Networks, 200*, 108488. https://doi.org/10.1016/j.comnet.2021.108488

Rosenfeld, M. (2012). Overview of colored coins, white paper. *Bitcoil co il, 41*, 94.

Saengchote, K. (2022). *Decentralized lending and its users: Insights from compound*. Available at SSRN 3925344.

Saggese, P., Belmonte, A., Dimitri, N., Facchini, A., Böhme, R. (2021). Who are the arbitrageurs? Empirical evidence from bitcoin traders in the mt. gox exchange platform. *arXiv preprint*arXiv:2109.10958.

Salehi, M., Clark, J., & Mannan, M. (2021). Red-black coins: Dai without liquidations. In *International Conference on Financial Cryptography and Data Security* (pp. 136–145). Springer. https://doi.org/10.1007/978-3-662-63958-0_12

Santoro, J. (2021). *Fei protocol: A decentralized, fair, liquid, and scalable stablecoin platform*. Tech. rep., Available at https://assets.fei.money/docs/whitepaper.pdf.

Sazandrishvili, G. (2020). Asset tokenization in plain English. *Journal of Corporate Accounting & Finance, 31*(2), 68–73. https://doi.org/10.1002/jcaf.22432

Schar, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. *Louis Review, 2*, 153–74.

Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. *arXiv preprint*arXiv:2107.10881.

Shin, H. S. (2022). *The great crypto crisis is upon us*. Available at https://www.ft.com/content/76234c49-cb11-4c2a-9a80-49da4f0ad7dd

Singh, A., Click, K., Parizi, R. M., & Zhang, Q. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications, 149*, 102471. https://doi.org/10.1016/j.jnca.2019.102471

Soska, K., Dong, J. D., Khodaverdian, A., Zetlin-Jones, A., Routledge, B., & Christin, N. (2021). Towards understanding cryptocurrency derivatives: A case study of bitmex. In *Proceedings of the Web Conference 2021 (WWW '21)*, 4. https://doi.org/10.1145/3442381.3450059

StakeDAO. (2022). *Documentation*. Available at https://stakedao.gitbook.io/stakedaohq/

Stifter, N., Judmayer, A., Schindler, P., & Weippl, E. (2022). Opportunistic algorithmic double-spending: How i learned to stop worrying and love the fork. In I. Part (Ed.), *Computer Security - ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings* (pp. 46–66). Springer. https://doi.org/10.1007/978-3-031-17140-6_3

Stroponiati, K., Abugov, I., Varelas, Y., Stroponiatis, K., Jurgeleviciene, M., & Savanth, Y. (2020). *Decentralized governance in defi: Examples and pitfalls*. DappRadar: Technical report.

Sushiswap. (2022). *Documentation*. Tech. rep., Available at https://docs.sushi.com/

Synthetix. (2022). *Synthetix litepaper*. Technical report. Available at https://docs.synthetix.io/litepaper/.

Thetanuts Finance. (2023). *Documentation*. Available at https://docs.thetanuts.finance/.

Tolmach, P., Li, Y., Lin, S. W., & Liu, Y. (2021). Formal analysis of composable DeFi protocols. In *International Conference on Financial Cryptography and Data Security* (pp. 149–161). Springer. https://doi.org/10.1007/978-3-662-63958-0_13

Twitter. (2021). Hacker hijacked true seigniorage dollar dao governance. Available at: https://www.reddit.com/r/CryptoCurrency/comments/m54w0t/hacker_hijacked_dao_governance_printed_himself/

von Wachter, V., Jensen, J. R., & Ross, O. (2021). Measuring asset composability as a proxy for DeFi integration. In *International Conference on Financial Cryptography and Data Security* (pp. 109–114). Springer. https://doi.org/10.1007/978-3-662-63958-0_9

Wang, Y., Chen, Y., Wu, H., Zhou, L., Deng, S., & Wattenhofer, R. (2022). Cyclic arbitrage in decentralized exchanges. In *Companion Proceedings of the Web Conference 2022*, WWW '22 (pp. 12–19). Association for Computing Machinery. https://doi.org/10.1145/3487553.3524201

Warren, W., & Bandeali, A. (2017). *0x: An open protocol for decentralized exchange on the ethereum blockchain*. Technical report. Available at: https://github.com/0xProject/whitepaper/blob/master/0x_white_paper.pdf

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

Wintermute, M. (2020). *Hegic: On-chain options trading protocol on ethereum powered by hedge contracts and liquidity pools*. Technical report. Available at https://crebaco.com/planner/admin/uploads/whitepapers/5261261Hegic.pdf

Wood, W. (2016). *Polkadot: Vision for a heterogeneous multi-chain framework*. Technical report. Available at https://polkadot.network/PolkaDotPaper.pdf.

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

Wood, G., et al. (2023). *The web3 foundation*. Available at https://web3.foundation/.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials, 22*(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706

Xu, J., Ackerer, D., & Dubovitskaya, A. (2021). A game-theoretic analysis of cross-chain atomic swaps with htlcs. In *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)* (pp. 584–594). IEEE. https://doi.org/10.1109/ICDCS51616.2021.00062

Xu, J., & Feng, Y. (2022). Reap the harvest on blockchain: A survey of yield farming protocols. *IEEE Transactions on Network and Service Management*. https://doi.org/10.1109/TNSM.2022.3222815

Xu, J., & Vadgama, N. (2022). From banks to DeFi: The evolution of the lending market. In *Enabling the Internet of Value*, pages 53–66. Springer. https://doi.org/10.1007/978-3-030-78184-2_6

Xu, T.A., & Xu, J. (2022). A short survey on business models of decentralized finance (DeFi) protocols. *arXiv preprint*arXiv:2202.07742

Xu, J., Paruch, K., Cousaert, S., & Sok, Feng Y. (2022). Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols. *ACM Computing Surveys, 55*(11), 1–50. https://doi.org/10.1145/3570639

Yearn Finance. (2020). *Yearn finance 3 - decentralized finance*. Technical report. Available at https://www.allcryptowhitepapers.com/wp-content/uploads/2020/12/YFI3.pdf.

Zargham, M., Shorish, J., & Paruch, K. (2020). From curved bonding to configuration spaces. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–3). IEEE. https://doi.org/10.1109/ICBC48266.2020.9169474

Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express, 6*(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001

Zhou, L., Xiong, X., Ernstberger, J., & Chaliasos, S. W. (2022). *Sok: Decentralized finance (DeFi) attacks*. Cryptology ePrint Archive, Paper 2022/1773, https://eprint.iacr.org/2022/1773

Authors and Affiliations

Raphael Auer[1] · Bernhard Haslhofer[2] · Stefan Kitzler[3] · Pietro Saggese[3] · Friedhelm Victor[4]

✉ Pietro Saggese
saggese@csh.ac.at

Raphael Auer
raphael.auer@bis.org

Bernhard Haslhofer
haslhofer@csh.ac.at

Stefan Kitzler
kitzler@csh.ac.at

Friedhelm Victor
friedhelm@trmlabs.com

[1] Bank for International Settlements, Basel, Switzerland

[2] Complexity Science Hub Vienna, Vienna, Austria

[3] Complexity Science Hub Vienna and AIT — Austrian Institute of Technology, Vienna, Austria

[4] TRM Labs, San Francisco, USA