Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols

Jiahua Xu and Yebo Feng

***Abstract*—Yield farming represents an immensely popular asset management activity in decentralized finance (DeFi). It involves supplying, borrowing, or staking crypto assets to earn an income in forms of transaction fees, interest, or participation rewards at different DeFi marketplaces. In this systematic survey, we present yield farming protocols as an aggregation-layer constituent of the wider DeFi ecosystem that interact with primitive-layer protocols such as decentralized exchanges (DEXs) and loanable funds (PLFs)protocol for loanable funds (PLF). We examine the yield farming mechanism by first studying the operations encoded in the yield farming smart contracts, and then performing stylized, parameterized simulations on various yield farming strategies. We conduct a thorough literature review on related work, and establish a framework for yield farming protocols that takes into account pool structure, accepted token types, and implemented strategies. Using our framework, we characterize major yield aggregators in the market including Yearn Finance, Beefy, and Badger DAO. Moreover, we discuss anecdotal attacks against yield aggregators and generalize a number of risks associated with yield farming.**

***Index Terms*—Decentralized finance (DeFi), yield farming, yield aggregator, simulation, blockchain.**

I. INTRODUCTION

YIELD farming protocols are deemed as the decentralized asset managers on blockchain. After having absorbed crypto assets from users—including both retail and institutional investors, yield farming protocols algorithmically deploy those funds into one or more revenue generating services such as lending and market making. Yield farming protocols have become immensely popular as they seem to create a win-win-win situation: users can earn return on their idle funds through an automated process; yield farming protocols can charge a management fee; other DeFi services can gain more liquidity.

The concept of yield farming was first popularized in mid 2020 by the leading PLF Compound with the introduction of its governance token `COMP` [92]. Compound participants get rewarded with newly-minted `COMP` tokens through both lending and borrowing activities, which lead to offsetting some loan costs for borrowers and increasing the return for lenders. This incentive scheme was quickly adopted by other protocols such as Uniswap [121] and Yearn Finance [70]) to attract liquidity and participation. As such, on top of the inherently designed benefit that users get for providing liquidity in different kinds of pools (e.g., interest in the case of lending protocols, or fees in the case of providing liquidity in automated market maker (AMM) pools), additional governance tokens are rewarded to users to further encourage their participation in the issuing platform during the early stage of adoption. The basic yield farming idea was born: the search for opportunities in the DeFi ecosystem to generate returns on otherwise dormant crypto assets.

TABLE I
TOP YIELD AGGREGATORS—MARKET SHARE INFORMATION

Yield aggregators	Governance token	TVL (m USD)	MCap (m USD)	Time established	Tokenholders
Yearn Finance	YFI	652.07	354.96	07/2020	49,668
Beefy	BIFI	302.95	39.00	09/2020	25,737
Badger DAO	BADGER	107.22	47.83	11/2020	30,757
Idle Finance	IDLE	94.17	1.38	11/2020	3,728
Yield Yak	YAK	72.13	3.56	09/2021	2,208
Autofarm	AUTO	64.99	26.52	02/2021	65,074
Flamincome	FLAG	59.55		06/2020	43
Rari Capital	RGT	47.03	64.27	07/2020	6,438
Vesper	VSP	42.62	4.35	02/2021	8,690
Spool Protocol	SPOOL	39.42	3.99	12/2021	522
Harvest Finance	FARM	32.74	37.39	09/2020	13,867
ACryptoS	ACS	30.09	2.06	12/2020	8,078
Reaper Farm	OATH	18.21	9.25	07/2021	2,993
Pickle Finance	PICKLE	14.20	1.49	09/2020	8,161
OnX Finance	ONX	4.63	1.41	03/2021	2,941
Waterfall DeFi	WTF	4.08	1.74	11/2021	852
Solidex	SEX	3.86	0.19	02/2022	9,389
Robo-Vault		3.81		07/2021	
Magik Farm	MAGIK	3.57		01/2022	2,110

Data fetched on 14/08/2022 from https://defillama.com/ - Yield Aggregators.

As a reaction to the creation of a multitude of platforms returning interests, fees and token rewards, yield aggregators—represented by Yearn Finance, Beefy, and Badger DAO (Table I)—dedicated to farming yield through DeFi primitives emerged. At the beginning 2021, the total value locked (TVL) of DeFi yield aggregators was still shy of 1 billion USD; by May 2021, however, this value grew exponentially to 8 billion USD (illustrated in Figure 1).

In this paper, we present a systemic examination of yield farming protocols. We first inspect yield farming protocols from the perspective of DeFi architecture and posit them as an aggregation-level component that interact with lower-level primitives in DeFi (see Section II). We then synthesize an action-state framework of yield farming operations, and extract yield farming protocols' features such as pool structure and accepted token types as well as their variations (see Section III). With our established model framework, we characterize top yield

Manuscript received 13 September 2022; revised 13 November 2022 and 14 November 2022; accepted 14 November 2022. Date of publication 16 November 2022; date of current version 7 March 2023. The associate editor coordinating the review of this article and approving it for publication was A. Veneris. *(Corresponding author: Yebo Feng.)*

Jiahua Xu is with the Computer Science Department, University College London, WC1E 6EA London, U.K. (e-mail: jiahua.xu@ucl.ac.uk).

Yebo Feng is with the Computer and Information Science Department, University of Oregon, Eugene, OR 97403 USA (e-mail: yebof@uoregon.edu).

This article has supplementary downloadable material available at https://doi.org/10.1109/TNSM.2022.3222815, provided by the authors.

Digital Object Identifier 10.1109/TNSM.2022.3222815

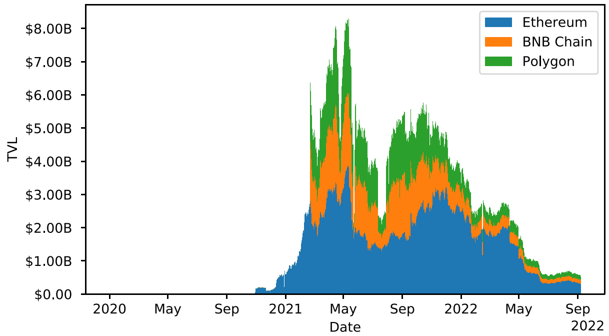


Fig. 1. TVL (b USD) of yield aggregators on Ethereum, BNB Chain and Polygon. Data collected on 12 September 2022 from https://defillama.com/.

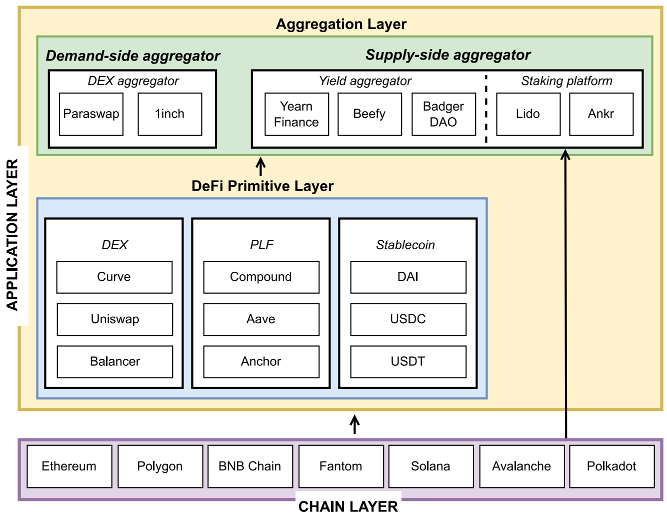


Fig. 2. Architecture of the DeFi ecosystem on blockchain.

farming protocols such as Yearn Finance, Harvest Finance and Pickle Finance. We argue that yield farming protocols are still associated with both security and economic risks (see Section IV) and provide a through literature review for interested readers (see Section V). In Appendix, in the supplementary material, we present simulations on three typical yield farming strategies in Section V-A, and describe the workings of top yield aggregators comparatively in Section V-B. Of a particular note here is that this paper is an updated and extended version of work published in [69].

II. Background in DeFi

Yield farming protocols are a constituent part of the wider DeFi ecosystem, and operate heavily dependent on other ecosystem components. In this section, we present those related components to understand where yield farming protocols reside within the DeFi ecosystem (illustrated in Figure 2).

A. DeFi Overview

Built on top of decentralized blockchain networks, DeFi [128] systems allow various financial products and services, including lending and asset trading, to be available to the general public. Compared with traditional financial systems, DeFi democratizes finance by replacing legacy, centralized institutions with algorithm-backed protocols, thereby improving the accessibility, inclusion, and transparency of financial services [99], [120].

B. Chain Layer

The distributed ledger technology (DLT) layer forms the infrastructural basis for decentralized applications (dApps). Like all other dApps, DeFi protocols consist of one or more smart contracts deployed on blockchain. To this end, the DeFi chain layer typically requires compatibility with smart contracts. As the oldest and the most widely adopted DLT that supports smart contracts, the Ethereum blockchain is also home to the majority of DeFi protocols [74]. The blockchain implements Ethereum Virtual Machine (EVM) to ensure that state transitions follow the same rules regardless of node they are performed on. The energy consumption and scalability issues associated with blockchains (e.g., EthereumPoW) that are based on the legacy proof of work (PoW) [104] prompted the emergence of the new Ethereum 2.0 and other EVM-compatible chain layer solutions such as Polygon [106], BNB Chain [65], Fantom [78], and Avalanche [60]. Those solutions incorporate alternative consensus mechanisms like proof of stake (PoS) and exhibit an improved throughput capacity [101]. PoS chains in particular not only provides the architectural foundation for the DeFi ecosystem, but can also be a source of yield: to encourage users' participation in the consensus of the distributed network, many of these PoS chains—including Ethereum 2.0 [77], Solana [116] and Polkadot [105]—reward users' staking activities.

C. DeFi Primitive Layer

Serving as the fundamental building blocks of the application layer of the DeFi ecosystem, DeFi primitives include AMM-based DEXs, PLFs and stablecoins. DeFi yield mainly comes from AMM-based DEXs and PLFs.

1) AMM-Based DEX: Different from order book-based exchanges where a trade has both buy and sell sides, AMM-based exchanges—often simply referred to as AMM—leverage an algorithm termed "conservation function" to determine the swap rate between two assets given the swap tokens and size [130]. As illustrated in Figure 3(a), traders using an AMM-based DEX swap their tokens against the exchange protocol's liquidity pool, which contains tokens deposited by liquidity provider (LPs). Against their funds contributed, LPs receive "LP tokens" as a form of "I owe you" (IOU), which allow liquidity withdrawal and entitle LP for their share of swap fee income. At the time of writing this paper, most prominent AMM-based DEX include Uniswap [122], Curve [71] and Balancer [61].

2) PLFs: A PLF (illustrated in Figure 3(b)) typically applies a pre-coded interest rate model that dynamically adjusts the borrow and supply rates [100]. Both rates are commonly programmed to positively correlate with the utilization ratio of the funds, defined as the total amount borrowed as a fraction of the total amount supplied for each specific token asset. PLFs on blockchain are mostly collateral-based rather than credit based. This means that a borrow position can only be created when a sufficient amount of deposit is in

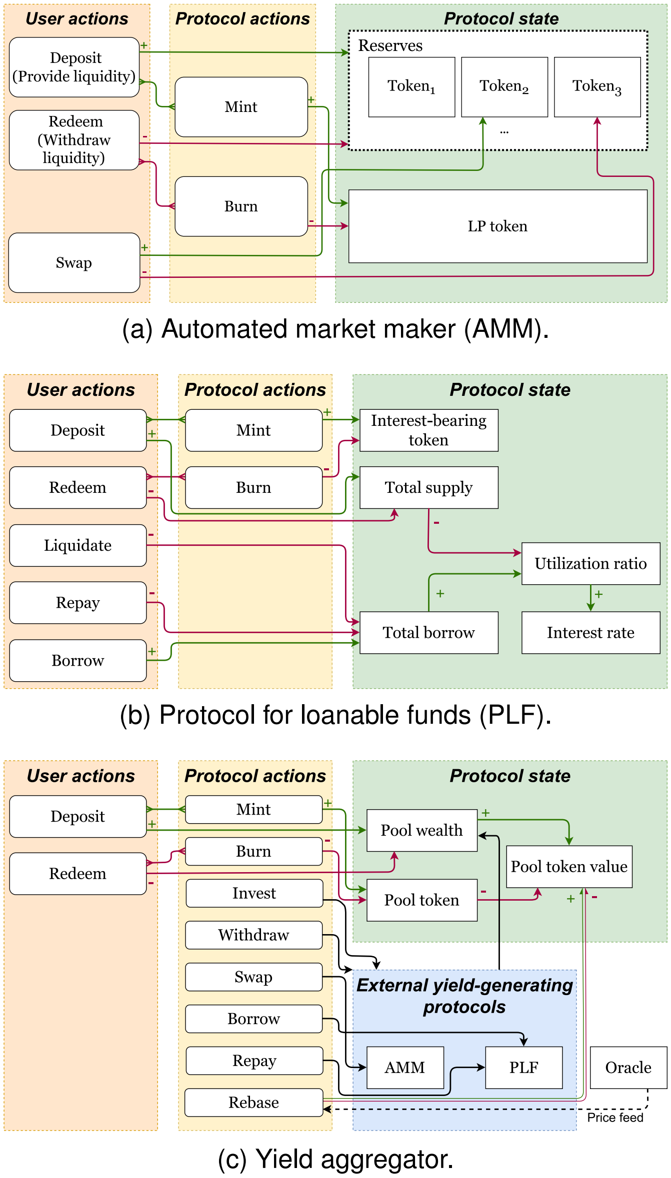


Fig. 3. State diagram with describing the interaction between the environment of a DeFi protocol and associated actions. + means positive effect, − negative effect.

place acting as collateral. The collateral might become liquidated if market movements or interest accrual cause the borrow position to become insufficiently collateralized. From the accounting perspective, interest accrual is achieved through "interest-bearing tokens" which, while sitting in their holder's wallet, increase in value with the passage of time. Analogous to AMM's LP tokens, interest-bearing tokens also serve as a from of IOU, which are emitted to lenders according to funds supplied and must be surrendered upon funds withdrawal. Aave [55] and Compound [67] can be counted as the two most popular PLF at the time of writing this paper.

3) Stablecoins: Stablecoins are token contracts deployed on blockchain representing cryptocurrencies that offer price stability relative to a certain reference asset [98], namely, a "peg". The peg can be another cryptocurrency, legal tender, commodities, or a combination of the above. At the time of writing this paper, the biggest stablecoins, `USDT`, `USDC` and `DAI` are all pegged to the US Dollar. Stablecoins can be custodial or non-custodial, asset-backed or algorithmically programmed.

D. Aggregation Layer

DeFi protocols on the aggregation layer interact with the chain layer or the DeFi primitive layer on end users' behalf [115]. Depending on whether their target users are requesting or providing services, aggregation layer protocols can be classified as demand-side aggregators and supply-side aggregators. The latter is the category the yield farming protocols belong to.

1) Demand-Side Aggregators: Channeling similar services offered by DeFi primitives, demand-side aggregators seek to present users with the most competitive offer so that they do not have to manually perform the comparison themselves. DEX aggregators Paraswap [37] and 1inch [1] algorithmically search for the optimal swap route through multiple primitive DEXs to generate the best exchange rate for users.

2) Supply-Side Aggregators: All supply-side aggregators to a certain extent perform some form of yield farming. Some protocols farm yields directly from the chain layer. For instance, staking platforms like Lido [93] and Ankr [57] act as a one-stop shop for users to benefit from staking rewards from various PoS chains; yield aggregators like Yearn Finance [134], Beefy [12] and Badger DAO [10] collect users' funds, redeposit them to DeFi primitives such as DEXs and PLFs or other aggregators to generate returns that will be re-distributed back to the users (presented in Figure 3(c)).

III. Yield Farming Preliminaries

In this section, we dive deep into the workings of yield farming protocols, understand how they generate yield for the users as well as revenue for the protocols themselves.

A. Types of Yield Farming Protocols

There is no universal definition for yield farming protocols. Some equate yield farming protocols to generic yield-generating protocols, in which sense, DeFi primitives such as AMMs and PLFs would also be counted as they offer yield to LPs and lenders, respectively. More commonly, however, yield farming protocols refer to protocols on the aggregation layer (see Section II-D) that pool funds to generate return by interacting with DeFi primitives. This is the type of yield farming protocols that we focus on in this paper.

Besides yield aggregators which are the most widely recognized type of yield farming protocols, some other protocols are more implicit in their farming activities by branding themselves as, e.g., stablecoin or lottery protocols. Those protocols mainly differ in the form of IOU tokens they mint to end users upon new deposit.

1) Yield Aggregators: Represented by Yearn, Beefy and Badger, the most classic and commonly known yield farming protocols are yield aggregators. In return for deposit into a yield farming pool, pool tokens that represent a fraction of the pool wealth are issued. Typically, the value of a pool token varies according to the total pool wealth (see Section III-B2h).

2) Yield-Bearing Stablecoins: A yield-bearing stablecoin protocol works similar to a savings account with a bank. Instead of minting pool tokens, the protocol issues stablecoins to users as a form of certificate of deposit. The yield-generating nature of the protocol is reflected in the increase in the quantity of the stablecoins to their holders, as opposed to the value of the stablecoin token; the value is designed to remain stable to the peg. `OUSD` issuer Origin Dollar and `USDi` issuer Bank of Chain [62] are two examples of this type of protocols.

3) Lottery Protocols: A lottery protocol collect users' funds and issue them each a lottery ticket token in return. The protocol then performs yield farming under the hood. Instead of distributing yield proportionate to users' deposit, the protocol every once in a while randomly selects one or more winners who can pocket the yield of all participants. PoolTogether [107] is one of the most popular protocols of this type while writing this paper.

4) NFT Farming: Recently, with the popularity of non-fungible token (NFTs), groups began to explore involving NFTs in yield farming. The main goal of NFT farming is to create liquidity and utility for NFTS, especially in gaming space, thereby earning yields for token owners [64]. Axie Infinity [52], ZooKeeper [136], Pulsar Farm [54], and MOBOX [53] are typical platforms that provide NFT farming services.

B. Yield Farming Operations

As illustrated in Figure 3(c), the entire yield farming process comprises actions from both the user and the protocol sides. We discuss common action types associated with yield farming protocols. The exact name and implementation of actions may deviate from one protocol to another.

1) User Actions: The actions that yield farming users, a.k.a "farmers", need to take are often trivial and straightforward.

a) Deposit: Protocol users simply select their favored yield farming pool and deposit their funds by transferring token assets to the pool smart contract. In return, users receive pool tokens as a form of IOU which should increase in value with the passage of time due to the yield farmed by the protocol [100], [130].

b) Redeem: Unless there is a timelock, users can redeem their deposited funds plus any yield generated anytime by surrendering their pool tokens.

2) Protocol Actions: The more sophisticated operations are assumed by the algorithm of the protocol where the actual yield farming is performed automatically under the hood.

a) Mint: The protocol mints pool tokens to the user proportionate to the amount of funds deposited, representing their share of the liquidity within the yield farming pool.

b) Burn: When a user requests to withdraw funds from a yield farming protocol, pool tokens need to be surrendered by the user and consequently burned by the protocol.

c) Invest: Depending on the DeFi primitive that the yield farming pool interacts with, the yield farming protocol can invest funds collected from users either into an AMM as a liquidity provider to collect swap fees (see Section III-B2c), or into a PLF as a lender to earn supply interests (see Section III-B2a). A yield farming pool may also invest in another yield farming protocol, often for the benefit of receiving reward tokens.

d) Withdraw: When end users request to redeem their funds from a yield farming pool, the pool contract needs to withdraw the corresponding amount of liquidity from the protocol(s) that it has invested in.

e) Swap: "Raw yield" does not always come in the form of the originally deposited assets. Therefore, the yield farming protocol may perform a swap, usually on an AMM, to convert yield tokens into the same tokens as originally deposited, which are sometimes reinvested to achieve the compounding effect.

f) Borrow: Yield farming protocols may use all or part of the funds deposited by users as collateral to borrow from a PLF. This may need to be performed due to various reasons: (i) to arbitrarily inflate the borrow position to be qualified for more participation reward (see Section III-B2b), (ii) to borrow out assets that can be invested to generate higher yield than the deposited assets.

g) Repay: Yield farming protocols that take the "borrow" action may need to partially or fully repay their loans to reduce or close its borrow position if: (i) the borrow position is on the verge of becoming liquidated, (ii) the collateral must be withdrawn so that it can be invested elsewhere or returned to end users.

h) Rebase: A yield farming pool mints or burns pool tokens depends on the quantity of the asset deposited or withdrawn as well as the exchange rate between the pool token and the asset. As yield farming progresses, the farming pool usually accumulates wealth and the exchange rate changes. Due to diversified investment in various protocols, some yield farming pools may possess an array of assets different from the one deposited by end users. Yield farming protocols connect to price oracles to fetch the price of each of these assets, and subsequently calculate the total value held by the pool. The exchange rate can thus be updated through dividing the latest pool value denominated by the asset deposited by end users with the circulating quantity of the pool tokens. This process of updating the pool token price is termed "rebase".

C. Forms of Yield Farming Pools

Different yield farming protocols vary in terms of their pool structure and token types acceptable by each pool (Table II).

1) Pool Structure: A yield farming pool may accept deposits in single or multiple assets.

a) Single asset: Most yield farming protocols have single-asset pools. While those pools only accept one particular token asset, they may still hold various assets due to different sorts of yield farmed. Typically, those other assets are automatically swapped for the one acceptable as deposits, and reinvested to generate compounded yield (see Section III-B2).

b) Multiple assets: A yield farming pool may also accept multiple token assets. Usually assets acceptable by the same pool share a peg. For example, at the time of writing this paper, Badger DAO's `ibBTC`/`crvsBTC` pool

TABLE II
TOP YIELD AGGREGATORS—PROTOCOL MECHANISM

		Pool structure		**Accepted token type**			**Strategies**			
Yield aggregators		Single asset	Multiple assets	Stablecoins	LP token	Others	Simple lending	Leveraged borrow	Liquidity provision	Chains
Yearn Finance	[49]	●	○	●	●	●	●	●	●	Ethereum, Fantom
Beefy	[12]	●	○	●	●	●	○	●	●	Polygon, Fantom, BNB
Badger DAO	[10]	●	●	○	●	●	●	○	●	Ethereum, Fantom, Polygon, BNB
Idle Finance	[31]	●	○	●	●	○	●	○	○	Ethereum, Polygon
Yield Yak	[50]	●	○	●	●	●	●	●	○	Avalanche
Autofarm	[9]	●	○	●	●	○	●	○	●	BNB, Polygon
Flamincome	[24]	●	○	●	●	○	○	○	●	Ethereum
Rari Capital	[39]	●	●	●	○	●	●	○	○	Ethereum
Vesper	[47]	●	○	●	○	●	●	○	●	Ethereum, Avalanche, Polygon
Spool Protocol	[45]	●	○	●	○	○	●	●	●	Ethereum
Harvest Finance	[30]	●	●	●	○	●	●	○	●	Ethereum, Polygon, BNB
ACryptoS	[4]	●	○	●	●	●	○	○	●	BNB, Fantom
Reaper Farm	[40]	●	●	●	●	●	○	○	●	Fantom
Pickle Finance	[38]	●	○	●	●	●	○	○	●	Ethereum, Polygon
OnX Finance	[34]	●	○	●	●	●	○	○	●	Ethereum, Polygon, Fantom, Avalanche
Waterfall DeFi	[48]	●	●	●	●	●	●	●	●	Avalanche, BNB
Solidex	[44]	●	○	●	○	●	○	○	●	Fantom
Robo-Vault	[42]	●	○	●	●	○	●	○	●	Fantom, Avalanche, Polygon
Magik Farm	[32]	●	○	●	●	●	○	○	●	BNB, Avalanche, Fantom

Data fetched on 28/08/2022 from corresponding documents.

accept `ibBTC`, `renBTC`, `WBTC` and `ibbtc/sbtcCRV-f`, all pegged to `BTC`.

2) Accepted Token Types: Yield farming protocols accept various types of tokens, ranging from stablecoins to LP tokens.

a) Stablecoins: In the recent low-interest environment in the traditional finance (TradFi) space, yield farming solutions that boast to offer a high single-digit to a double-digit annual percentage yield (APY) for USD-pegged stalecoins have been of particular interest. Most yield farming protocols offer stablecoin farming; in fact, among the top 20 yield aggregators, only Badger DAO has no stablecoin pool thus far.

b) LP tokens: Many yield farming pools also accept LP tokens. As discussed in Section II-C1, LP tokens themselves already entitle their tokenholders to swap fee income. Nevertheless, having LP tokens managed by a yield farming pool provides the additional benefit of automatically converting and reinvesting participation reward (see Section III-D3) distributed by the respective AMM.

c) Others: Other asset types may also be eligible for yield farming. For example, Yearn Finance accepts `ETH`, the native currency on the Ethereum blockchain, as well as `UNI` and `YFI`, which are protocol governance tokens of Uniswap and Yearn Finance itself, respectively.

D. Sources of Yield

1) Supply Interest: The most straightforward type of yield originates from lending. As the demand for loans in crypto assets grows, the borrowing interest rate increases, leading to higher yields for lenders. Particularly in a bullish market, speculators are keen to borrow funds despite a high interest rate, in expectation of an appreciation in the assets of their leveraged long position. A borrower wishing to increase their exposure to `ETH`, for example, may use `ETH` as collateral to borrow `USDC`, then repetitively exchanging `USDC` for `ETH` to deposit it as collateral to borrow more `USDC`, forming a "leveraging spiral" [131]. Compound [67] and Aave [55], two major DeFi lending protocols while writing this paper (see Section II-C2), have witnessed the borrow APY of `USDC` rising from 2-3% in May 2020 to as high as 10% in April 2021.[1] This specific kind of yield is incorporated in interest-bearing tokens, such as `cTokens` from Compound or `aTokens` from Aave.

2) Swap Fee Income: Some tokens entitle users to part of the revenue that is going through the protocol. These can be governance tokens or other kinds of tokens. One example is the liquidity provider tokens in AMM-based DEXs [130]. By supplying liquidity into an AMM pool, users receive the fees that are paid by traders within that pool. The higher the volume in that pool, the more fees that are generated, and the more a liquidity provider profits from this. In Uniswap [122], a 0.3% fee is charged for every trade within a pool and goes fully to LPs.

3) Participation Reward: Another yield source comes from liquidity mining programs, where early participants receive native tokens representing protocol ownership. This incentivizes people to contribute funds into the protocol, and enhances decentralization as the protocol ownership is distributed to users. The native tokens often have a governance functionality attached to them which is deemed valuable, as the token holders have a say in the future strategic direction of the project. Native tokens sometimes also entitle holders to a share of the protocol revenue. Further, the values these tokens possess itself especially in a speculation context can be the benefits of owing a protocol.

This brings up a second kind of revenue-sharing token, where users have to actively stake their tokens to receive a share of the revenue. For example, `SUSHI` holders that stake their `SUSHI` will get `xSUSHI` in return, which represents the proportional share of a pool that captures 0.05% of all trades on Sushiswap [117]. Vesper Finance's governance token, `VSP`, can also be deposited in a pool, in return for `vVSP`, a token that represents the user's proportional share of a pool that captures part of the revenue generated throughout the whole Vesper platform [124].

[1] https://app.defiscore.io/assets/usdc

TABLE III
OVERVIEW OF ATTACKS IN AGGREGATORS AND POTENTIAL SOLUTIONS

Attacks	Yield aggregator attacked	Summary	Solutions	Estimated lost	References	Time	Major chain
Flash loan attack	ApeRocket	Using the fact that the AutoCake vault was only deployed 10 hours and was low in TVL, attacker conducted price manipulation and drained the vault.	Project team updated the protocol and at least two audits will be conducted before its V2 launch.	1.26 m USD	[18], [6], [7]	07/14/2021	BNB
	Pancake Bunny	Within the timeframe to create a new block, attacker transferred USDT into the contract and called removal of liquidity. Caused the value of Bunny token to crash by more than 95%.	A implementation of the Floating Rate of Emissions and the security code changes.	3 m USD	[35], [36], [25], [27], [23]	05/20/2021	BNB
	Harvest Finance	Attacker swapped USDC to USDT to up the price of USDT, depositing USDT into vault and swap back USDT to USDC to gain profit as USDT price fall. This action is repeated to drain the vault.	Team updated the following: deposit and withdraw funds within a single transaction is not allowed to avoid flash loan, and withdraw of tokens are made into multiple transactions to minimize damage.	33.8 m USD	[28], [29], [51]	26/10/2020	Ethereum
Rug pull	Arbix Finance	The project team drained the vault with users assets, deleted their website, twitter and telegram.	Certik sent out a community alert.	10 m USD	[8], [43]	01/04/2022	BNB
Reentrancy attack	ForceDAO	The xFORCE platform used a fork of xSUSHI contract which revert the token if transaction fails, they also used Aragon Minime token that return false if a transferForm() call fails.	Team could have used a standard Open Zeppelin ERC-20 or added a safe transferFrom wrapper in xSUSHI contract.	367 k USD	[21], [17]	04/03/2021	BNB
	Grim finance	Attacker exploited a depositFor() function that had not been protected. Users deposited funds in to vaults that attacker inserted their own contract containing the reentrancy deposit loops.	The team updated the code and send in for an audit.	30 m USD	[5], [2], [26], [22]	19/12/2021	Fantom
	DAO Maker	The init() function was vulnerable, attacker initialized 4 token contracts with malicious data then used the emergencyExit() function to drain funds.	The source code is not public so protecting and checking the project is a priority. Also to fix the vulnerability in the function.	4 m USD	[16], [15]	09/03/2021	Ethereum
	Reaper Farm	Attacker took advantage of that the recipients account verification had not been set up properly and drained the vault.	The project team closed down the vaults attacked, altered the code and waiting for full audit before launching again.	1.7 m USD	[41], [33], [3]	01/08/2022	Fantom
Key exploit	Bent Finance	The contract used a non multisig wallet, allowing anyone that knows the private key to modify updates, which caused the attacker to create a back door. Attacker altered the code so that Bent finance would provide large amount of funds to the attacker's address.	Project team could have used multisig wallet to avoid and protected private keys in an appropriate way.	1.75 m USD	[13], [14], [20]	12/21/2021	BNB
	Badger DAO	Attacker used a compromised API key to periodically inject malicious code into the contract. These codes are triggered when users try to perform transactions, allowing unlimited spend approvals for the attacker's address.	Project team working with cybersecurity firm to fix the problem, as well as authorities to recover any funds possible.	120 m USD	[11], [46], [19]	02/12/2021	BNB

E. Revenue Model of Yield Farming Protocols

Yield farming protocols often retain a fraction of yield earned as the protocol revenue [132]. In the spirit of Decentralized Autonomous Organization (DAO), the revenue may be redistributed to tokenholders of the protocol governance token [133]. In that sense, a stronger buy pressure of a particular governance token of a yield farming protocol usually mirrors a larger (anticipated) TVL of the protocol, as it can translate to higher protocol revenue.

IV. YIELD FARMING RISKS

Compared with asset management in traditional finance (TradFi), yield farming may bring substantial profits in short order but also carry a range of risks.

A. Security Risks

We identify four major types of attacks associated with yield farming. Table III presents anecdotal events of these attacks and their potential solutions.

1) Flash Loan Attack: Flash loan attacks [110] abuse the mechanism of flash loan protocols in which an attacker borrows a great deal of funds that do not require collateral. The attacker then manipulates the price of an asset in a very short period and quickly resell it to earn profits. Such a procedure can be repeated for multiple time by the attacker, thereby causing considerable losses to investors and yield aggregators.

Major yield aggregators have witnessed multiple waves of flash loan attacks, losing millions of dollars each. For example, ApeRocket suffered two flash loan attacks that costed investors 1.26 million USD on July 2021 [18]; in October 2020, a farmer leveraged flash loans to reap 33.8 million USD from the `USDT` and `USDC` pools [28]; Pancake Bunny Finance lost around 690,000 `BUNNY` tokens due to removal of liquidity and price manipulation by flash loan attacks [35].

To defend against flash loan attacks, developers must consolidate and improve flash loan protocols, making them difficult to be exploited by attackers. An effective approach is to setup floating interest rates, thereby increasing the cost of launching flash loan attacks [35]. Developers can also choose to enhance the audits [7] or forbid depositing and withdrawing funds within a single transaction [51].

2) Rug Pull: A rug pull refers to the abandonment of a project by the project administrator after collecting investor's funds, leaving investors with valueless assets [118], [130]. One way of conducting this type of scam is to lure yield farming protocols into buying assets with no value and then swap this asset for `ETH` or another type of asset with value. For example, Arbix Finance, a typical rug pull, drained around 10 m USD in users' assets directly from the vaults without any advanced attack techniques in sight [8].

To prevent from being rugged, investors should exercise caution and always confirm a project's credibility before investing in it [95], [129]. Besides, continuously tracking the audit information of invested projects enables investors to quickly identify risks and take appropriate measures, thereby reducing losses [43].

3) Reentrancy Attack: Even though the composability factor of DeFi is what makes yield farming possible in the first place by allowing for complex, interconnected financial protocols, it does bring along the danger of smart contract risk as more and more money legos are plugged into a strategy. While two smart contracts may be secure in isolation, the combination of them may not. By composing multiple smart contracts together, the attack surface might be greater than the sum of its parts [126], [127].

Reentrancy attack is one of the most destructive attacks that appear when multiple smart contracts operate with each other. More specifically, the reentrancy attack occurs when a smart contract makes an external call to another smart contract. Then the another contract makes recursive calls back to the original function, intentionally or unintentionally withdraw funds. When the original contract fails to update its state before sending funds, the attacker can exploit this vulnerability to continuously drain the contract's funds.

Major yield aggregators have witnessed a large amount of reentrancy attacks in the past several years. In April 2021, the ForceDAO DeFi aggregator was exploited by a group of attackers, who utilized reentrancy attacks to steal 367 thousands USD worth of tokens before the ForceDAO team took effective actions to prevent further attacks [19]; in September 2021, DAO Maker, a decentralized finance platform on Ethereum, was hacked for almost 4 million USD due to insecure smart contracts [16]; a reentrancy attack on the Grim Finance project within the Fantom Blockchain also successfully drained over 30 million USD worth of tokens in 2021 [5].

To defend protocols against reentrancy attacks, researchers and developers have proposed a variety of frameworks and methods [86]. For example, Rodler et al. [112] propose a backward compatible approach based on run-time monitoring and validation to protect smart contracts on Ethereum; Das et al. [73] propose a reentrancy-aware language called Nomos, which enforces reentrancy security using resource-aware session types; Cecchetti et al. [66] first formalize the reentrancy interface on general distributed systems and then leverage information flow control to automatically fix defective smart contracts. However, with the increasing complexity and variety of DeFi protocols, reentrancy attacks will also become increasingly difficult to detect and counter. From users' side, protection can be sought from DeFi-native insurance protocols such as Nexus Mutual that cover smart contract risks [68].

4) Key Exploit: Due to poor access control of some DeFi systems, yield aggregators can be attacked by exploiting various keys (e.g., API key, wallet key) to tamper with the smart contracts or drain funds. For example, the Bent Finance utilized non-multisig wallets to deploy their project's smart contracts. Anyone who knows the appropriate private key can perform updates to the contracts, allowing attackers to inject malicious code and create the backdoor. In December 2021, an attacker leveraged this feature to drain 1.75 million USD worth of tokens from the pool [13], [14], [20].

To avoid attacks based on key exploiting, DeFi contracts should always be deployed upon multisig wallets to eliminate single points of failure [20]. DeFi platforms should also properly protect the private keys used to access and control correlative smart contracts. The developments of DeFi system API, application, and user interface should follow software security practices, ensuring that the access control and function calls are solidly implemented.

5) Other Attacks: As yield farming protocols are built upon multiple complex systems with a variety of software and hardware components interacting with each other, both technical and economic weaknesses give rise to attractive exploit opportunities for malicious hackers. Besides the aforementioned attacks, there are many other attacks targeting the blockchain infrastructure, user interface, or even network communications, thereby disturbing the proper operation of yield farming protocols. For example, malicious miners can prioritize transactions in their favor by inspecting maximal extractable value (MEVs), thereby causing damages to the smart contracts running on the upper layers [109], [135]; attackers can break the network connections between the users and the blockchain system through border gateway protocol (BGP) hijacking [58]; malicious traders can leverage front-running attacks to drain funds from pools [76].

These attacks are out of scope for this paper, but it is important for users and developers to be aware of that yield farming security is a systemic problem. Only by ensuring the security of every component in the system can the security of yield seekers' funds be ensured.

B. Economic Risks

Besides security concerns, there exist various economic risks associated with yield farming. In Section **??**, we demonstrate that investment strategies with the potential to generate remarkably high yield also bear high risks. While our simulation only illustrate return courses in a deterministic fashion, through various simulated scenarios one can easily extrapolate that the ever-changing market conditions—including volatile price movements and trading activities—lead to return instability, and sometimes even losses. Below, we discuss several types of economic risks associated with yield farming.

1) Yield Dilution Risk: Yield farming pools providing double or even triple digit APY can be deceiving in their return generating capability. Often enough, those pools are thin in liquidity and lack scalability, unable to accommodate a large amount of deposit while sustaining a similar level of APY. Users who invest a significant amount of funds into such a pool may find the pool APY dropping significantly immediately afterwards. For users with funds already in the pool, they may experience a decrease in return on their investment due to dilution from newly added funds. For those who do not constantly monitor their investment performance, this may mean leaving their funds in a diluted, low-APY pool, while missing the opportunity of reallocating their funds to more profitable strategies.

2) Conversion Risk: As discussed in Section III-C, yield farming pools typically specify tokens that they can accept. Therefore, to participate in yield farming, users may have to first convert partially or all of their funds into acceptable assets for yield farming. This engenders conversion risk: a user might have been better off holding their original funds, than converting them to "eligible" assets. This is because the "eligible" assets might depreciate against the original assets prior to the conversion to such an extent that even the yield generated cannot make up for the depreciation loss. This risk is most prominent with liquidity provision strategies, manifested by the so-called "impermanent loss" (see [130]). By design, the value LP tokens (e.g., `USDT-ETH-LP` token) from an AMM-based DEX falls against the original portfolio (e.g., a combination of `USDT` and `ETH`). Sometimes, even the swap fee income and the participation reward are insufficient to cover the conversion loss.

3) Exchange Risk: Related to conversion risk, exchange risk is associated with the uncertainty surrounding the exchange rate between the assets held by the yield farming pool and the denominating currency (usually USD). As demonstrated in Section III-A2, yield farming strategies benefit from—and, in cases such as leveraged borrow, solely rely on—the high value of participation reward. This makes yield farming highly speculative as token prices are unpredictable. An overly low price of yielded tokens such as reward tokens might result in a loss for end users.

4) Counterparty Risk: This risk is associated with farming strategies that incorporate lending, where loans might not be repaid. While the simple lending strategy (see Section III-B2a) is a relatively low-risk one, losses may still occur under extreme market conditions, e.g., when the price of the asset lent out relative to the collateral suddenly increases to such a significant extent that the loan becomes undercollateralized (see lending protocol MakerDAO's Black Thursday Incident [91], [100]). In such cases, borrowers may choose not to repay their loans since their collateral is not worth the effort anymore, resulting in a default. Kao et al. [90] simulate a wide range of market volatility to stress-test lending protocols such as Compound, and find that only rarely can undercollateralization occur.

5) Liquidation Risk: Liquidation risk is associated with farming strategies such as leveraged borrow (see Section III-B2b) that incorporate taking a overcollateralized loan on a PLF. Due to price movements and interest accrual, a loan position may become insufficiently collateralized, triggering liquidation of the deposited assets backing the loan. At liquidation, the value of the collateral liquidated by design exceeds the loan payable reduced, resulting a loss on the side of the borrower. Thus, yield farming protocols that implement borrow but unable to handle liquidation risk properly may cause users to lose their funds.

V. Related Work

In this section, we introduce literature that is related to yield farming in some shape and form. As it is still a fairly new area, there is a paucity of existing works related to our paper. Table IV summarizes the most related and representative ones.

In general, our paper is different from existing papers in the following aspects:

- our paper focuses on the subject of yield farming, while other papers either investigate a more specific DeFi topic (e.g., yield generating mechanism [125], yield chasing [114]), examine a different but related DeFi applications (e.g., AMM-based DEX [130], lending [63]), or have a broader coverage (e.g., DeFi transformation [108]);
- to investigate yield farming comprehensively, our paper utilizes multiple methodologies, including literature survey, modeling, empirical analysis, and taxonomization. In contrast, other papers use only one or a few of these methodologies to study their subjects;
- our paper examines a series of aspects of yield farming, including related DeFi protocols, yield generation, yield farming strategies, financial risks, and security issues, while most of the related papers only cover some of these topics.

We discuss related literature in more details from different perspectives in the following subsections.

A. Yield Farming

A few papers focus on studying and comparing yield farming strategies or yield aggregators [59]. For instance, Walton [125] provides a break down of yield generating mechanism, covering four different farming strategies and a few other related topics (e.g., benefits and risks); Kanis Saengchote [114] studies DeFi composability, which covers yield-chasing behaviors and some introductions about major yield aggregators; another case study about Compound [113] also comes with explanations about yield aggregators and yield farming incentives; Popescu [108] discuss the transition from the traditional finance to DeFi and include some descriptions about yield farming.

However, none of these works have comprehensively investigated yield farming from the perspective of literature survey, modeling, empirical analysis, and taxonomization like our paper.

B. DeFi Platforms

As a type of DeFi application, yield farming is built upon DeFi platforms. Combing the design of general DeFi platforms lays the groundwork for yield farming designs. Moin et al. [98] and Pernice et al. [102] systematically study the general designs of DeFi platforms by decomposing the structure into diverse elements (i.e., peg assets, collateral amount, price and governance mechanism). They also investigate the merits and demerits of DeFi platforms to spot future directions. Nonetheless, yield farming is not the main focus of these works.

C. Related DeFi Protocols

There are various papers studying the DeFi protocols (e.g., flash loan, lending, trading) that can be leveraged by yield farming. For example, as fundamental protocols of yield farming, the mechanisms, properties, and risks of DeFi lending protocols are extensively investigated in several publications [63], [90], [100], [119]; some papers [81], [100] provide analysis and discussions about protocols for Loanable Funds, introducing the interest rate determination and liquidity issues; Han et al. [82] zoom into the launch event of the yield farming protocols for Uniswap liquidity provision and further establish

TABLE IV
OVERVIEW OF RELATED LITERATURE

Ref.	**Summary**	**Subjects Covered**			**Methodology**			
		Yield farming strategies	Major yield aggregators	Risk evaluation	Literature review	Modeling	Empirical analytics	Taxonomization
This paper	A survey that uses examples of yield strategies to compare the major yield aggregators, translating them into revenue models and empirical examinations supported with on-chain data.	●	●	●	●	●	●	●
[59]	A paper that characterizes the risk and return characteristics of yield farming investment strategies on PancakeSwap, one of the largest automated market makers among the emerging ecosystem of decentralized financial services.	●	◐	●	◐	●	●	○
[114]	A presentation of yield-chasing behavior adopting on-chain transaction level data and empirical analysis to support the result. The paper also classifies DeFi protocols including major yield aggregators.	●	●	○	○	○	●	●
[125]	A break-down of the mechanism of yield generating, also it provides an overview of four different strategies and other related DeFi services.	●	●	●	○	○	○	●
[91]	A case study assessing the stability of MakerDAO protocol, which uses public data and protocol analysis.	●	○	●	○	○	●	○
[113]	A case study about Compound with detailed explanation of how it works, and where it is applied.	●	●	●	○	○	●	◐
[82]	An analysis of impact on trading using data from Binance's and Uniswap's program in yield farming. It also compares their differences and evaluate how DeFi provides an alternative solution to the traditional finance.	●	○	●	○	○	○	●
[108]	A discussion of the transition from the traditional finance to DeFi and its advantages, covering methods of yield farming.	●	○	●	○	○	○	●
[131]	A presentation of the advantageous DeFi characteristics that would resolve a list of fundamental issues in the traditional lending system.	●	●	●	○	○	○	●
[63]	A systematic analysis on lending pools and their behavior, focuses on two specific lending platforms.	●	○	●	○	●	○	◐
[81]	A discussion of the Protocol for Loanable Funds, also reviews the methodology of interest rate determination and provides empirical examination corresponding to different degrees of liquidation.	●	○	●	○	●	○	●
[100]	An empirical analysis of liquidation on Protocol for Loanable Funds, focuses on Compound. The paper also provides calculation of liquidators efficiency and discusses the security issues and risks.	●	○	●	○	●	●	○
[98]	A discussion on the structure of stablecoins that breaks down existing stablecoins into components to compare and evaluates their advantages and disadvantages.	●	○	○	○	○	○	◐
[130]	An SoK on AMM based DEX protocols, compares the popular protocols mechanisms and discusses the securities and privacy concerns.	●	○	●	●	●	●	●
[96]	A discussion on the method of maximizing the discounted value of future returns and analyzes the geometric relationships between the expectation and the choice of portfolio.	○	○	●	○	●	○	◐

the causal impact of this on Binance investor trading activities; within the scope of the analysis of financial attack vectors that involve a flash loan, Qin et al. [110] study the existing flash loan-based attacks and propose optimizations that significantly improve the ROI of these attacks; Gudgeon et al. [80] explore how design weaknesses in DeFi protocols can trigger a decentralized financial crisis.

Although these papers can cover almost all the DeFi protocols used by yield farming, our paper presents this topic more systematically by putting together all the relevant protocols, components, and problems worth exploring.

VI. CONCLUSION

In this survey paper, we examine yield farming protocols from multiple perspectives. We first highlight yield farming's dependence on lower-level DeFi primitives in the context of the broader DeFi ecosystem and propose a general framework for yield farming protocols. We then explain code-level actions and associated yield farming operations. We decompose various aspects of yield farming protocols such as protocol form, pool structure, accepted token types, and enumerate their variations. Later, we stylize three frequently used strategies and simulate yield farming performance under a set of assumptions. We also compare four major yield aggregators by summarizing their strategies and revenue models. Finally, we discuss security and economic risks of yield farming protocols, together with related work.

While yield farming has been exploding since 2020, an important question remains if current yields will be sustainable in the long term. Higher rewards also imply higher risks, and associated DeFi attacks prove that the safest and most robust yield provider will win the race. Besides security enhancement, new industry developments should consider building one-stop-shop solutions, in pursuit of aggregating more than just yield and facilitating the on-boarding of new DeFi users.

ACKNOWLEDGMENT

The authors would like to extend their sincere thanks to Simon Cousaert and Toshiko Matsui for the base of this paper [69]. The authors also would like to thank Yitian Wang and Honglin Fu for their research assistance.

This material is based upon work partially supported by Ripple under the University Blockchain Research Initiative (UBRI) [79]. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Ripple.

REFERENCES

[1] "1Inch." Accessed: Nov. 12, 2022. [Online]. Available: https://app.1inch.io/#/1/unified/swap/ETH/DAI
[2] "$30 Million Stolen From Grim Finance, Audit Firm Blames New Hire for Vulnerability." Accessed: Aug. 15, 2022. [Online]. Available: https://www.zdnet.com/article/30-million-stolen-from-defi-protocol-grim-finance-audit-firm-apologizes-for-missing-vulnerability/
[3] "8/1/2022 Reaper Farm Exploit Recovery Plan." Accessed: Aug. 15, 2022. [Online]. Available: https://docs.google.com/document/d/1wymADZrvisr8UNU9BHWh9bgEsO28D2-awhOHlxlQ3X8/edit
[4] "ACryptoS Docs." Accessed: Aug. 15, 2022. [Online]. Available: https://docs.acryptos.com/
[5] "Analysis of the Grim Finance Hack." Accessed: Aug. 15, 2022. [Online]. Available: https://slowmist.medium.com/analysis-of-the-grim-finance-hack-bc440108b069
[6] "ApeRocket Finance Incident Analysis—Improper Reward Minting." Accessed: Aug. 15, 2022. [Online]. Available: https://inspexco.medium.com/aperocket-finance-incident-analysis-improper-reward-minting-52153a8958fa
[7] "ApeRocket Releases Official Statement Regarding 1.2 Million DeFi Hack." Accessed: Aug. 15, 2022. [Online]. Available: https://www.bsc.news/post/aperocket-releases-official-statement-regarding-1-2-million-decentralized-finance-defi-hack
[8] "ARBIX FINANCE—REKT." Accessed: Aug. 15, 2022. [Online]. Available: https://rekt.news/arbix-rekt/
[9] "Auto Farm Docs." Accessed: Aug. 15, 2022. [Online]. Available: https://autofarm.gitbook.io/autofarm-network/
[10] "Badger Dao Docs." Accessed: Aug. 15, 2022. [Online]. Available: https://badger-finance.gitbook.io/badger-finance/
[11] "BadgerDAO Reveals Details of How It Was Hacked for $120M." Accessed: Aug. 15, 2022. [Online]. Available: https://www.coindesk.com/business/2021/12/10/badgerdao-reveals-details-of-how-it-was-hacked-for-120m/
[12] "Beefy Finance Docs." Accessed: Aug. 15, 2022. [Online]. Available: https://docs.beefy.finance/
[13] "BENT FINANCE—REKT." Accessed: Aug. 15, 2022. [Online]. Available: https://rekt.news/bent-finance/
[14] "Bent Finance Confirms Pool Exploit, Advises Investors to Withdraw Funds." Accessed: Aug. 15, 2022. [Online]. Available: https://cointelegraph.com/news/bent-finance-confirms-pool-exploit-advises-investors-to-withdraw-funds
[15] "DAO MAKER—REKT." Accessed: Aug. 15, 2022. [Online]. Available: https://rekt.news/daomaker-rekt/
[16] "DAO Maker Hack." Accessed: Aug. 15, 2022. [Online]. Available: https://www.coinfirm.com/blog/dao-maker-hack/
[17] "DeFi Aggregator Raided by Five Hackers on Launch Day." Accessed: Aug. 15, 2022. [Online]. Available: https://cointelegraph.com/news/defi-aggregator-raided-by-five-hackers-on-launch-day
[18] "DeFi Yield Farming Aggregator ApeRocket Suffers $1.26M 'Flash Loan' Attack." Accessed: Sep. 1, 2022. [Online]. Available: https://uk.finance.yahoo.com/finance/news/defi-yield-farming-aggregator-aperocket-153230316.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADu5E7nD5fyENrdA94UutsadM6zSa9g9vpls75qherSwUpaqgCPM9uRMC7ay3-kqbOEDBkkfkMrEM-O4qBBtBPFdbdKu9w2kgVujSc44sNiQyUfvuoGHiAtDCNqyjG9Y9y_7PJwvGLh1snrEy2dvs0qCssx3ah4qaUYP-__DyR-S
[19] "Explained: The Badgerdao Hack (December 2021)." Accessed: Sep. 1, 2022. [Online]. Available: https://halborn.com/explained-the-badgerdao-hack-december-2021/
[20] "Explained: The Bent Finance Hack (December 2021)." Accessed: Sep. 1, 2022. [Online]. Available: https://halborn.com/explained-the-bent-finance-hack-december-2021/
[21] "Explained: The Forcedao Hack (April 2021)." Accessed: Sep. 1, 2022. [Online]. Available: https://halborn.com/explained-the-forcedao-hack-april-2021/
[22] "Explained: The Grim Finance Hack (December 2021)." Accessed: Sep. 1, 2022. [Online]. Available: https://halborn.com/explained-the-grim-finance-hack-december-2021/
[23] "Explained: The Pancakebunny Protocol Hack (May 2021)." Accessed: Sep. 1, 2022. [Online]. Available: https://halborn.com/explained-the-pancakebunny-protocol-hack-may-2021/
[24] "Flamincome Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.flamincome.finance/guide/terminal
[25] "Flash Loan Attack Causes DeFi Token Bunny to Crash Over 95%." Accessed: Sep. 1, 2022. [Online]. Available: https://www.coindesk.com/markets/2021/05/20/flash-loan-attack-causes-defi-token-bunny-to-crash-over-95/
[26] "GRIM Finance—Rekt." Accessed: Sep. 1, 2022. [Online]. Available: https://rekt.news/grim-finance-rekt/
[27] "Hack Track: Pancake Bunny Hack." Accessed: Sep. 1, 2022. [Online]. Available: https://medium.com/merkle-science/hack-track-pancake-bunny-hack-aaa62fe49313
[28] "Harvest Finance—Rekt." Accessed: Sep. 1, 2022. [Online]. Available: https://rekt.news/harvest-finance-rekt/
[29] "Harvest Finance: $24M Attack Triggers $570M 'Bank Run' in Latest DeFi Exploit." Accessed: Sep. 1, 2022. [Online]. Available: https://www.coindesk.com/tech/2020/10/26/harvest-finance-24m-attack-triggers-570m-bank-run-in-latest-defi-exploit/
[30] "Harvest Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://harvest-finance.gitbook.io/harvest-finance/
[31] "Idle Finance Doc." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.idle.finance/
[32] "Magik Farm Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://avery-bigweapon.gitbook.io/magik.farm-docs/
[33] "Multi-Strategy Vault Post-Mortem." Accessed: Aug. 15, 2022. [Online]. Available: https://docs.google.com/document/d/1aCEbz40BBC3y1RqDksnD9d-5IOXXgbeKAvJWMH2GoI4/edit
[34] "OnX Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://onx-finance.gitbook.io/docs/
[35] "PancakeBunny Releases Recovery Plan Post Flash Loan Attack." Accessed: Sep. 1, 2022. [Online]. Available: https://cryptodaily.co.uk/2021/06/pancakebunny-recovery-plan?utm_source=dlvr.it&utm_medium=twitter
[36] "Pancakebunny Security Code Change." Accessed: Sep. 1, 2022. [Online]. Available: https://smartliquidity.info/2021/05/22/pancakebunny-security-code-change/#more-13374
[37] "ParaSwap: Best Prices in Defi for Traders & Dapps," Accessed: Nov. 12, 2022. [Online]. Available: https://www.paraswap.io/
[38] "Pickle Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.pickle.finance/
[39] "Rari Capital Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.rari.capital/
[40] "Reaper Farm Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.reaper.farm/reaper-farms/faq-1/why-use-reaper.farm
[41] "Reaper Farm Just Lost US$1.7 Million From Exploit—Will It Be Able To Recover From This?" Accessed: Sep. 1, 2022. [Online]. Available: https://chaindebrief.com/reaper-farm-got-hacked/
[42] "Robo Vault Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.robo-vault.com/robovault/vaults
[43] "Rug Pull Alert: Arbix Finance (ARBX) Is a Scam." Accessed: Sep. 1, 2022. [Online]. Available: https://www.cryptopolitan.com/arbix-finance-is-a-rug-pull/
[44] "Solidex Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.solidexfinance.com/
[45] "Spool Protocol Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.spool.fi/technical-reference/understanding-the-protocol
[46] "The BadgerDAO Hack: What Really Happened and Why It Matters." Accessed: Sep. 1, 2022. [Online]. Available: https://zengo.com/the-badgerdao-hack-what-really-happened-and-why-it-matters/
[47] "Vesper Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.vesper.finance/
[48] "Waterfall DeFi Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://defi-waterfall.gitbook.io/waterfall-finance/
[49] "Yearn Finance Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.yearn.finance/
[50] "Yield Yak Docs." Accessed: Sep. 1, 2022. [Online]. Available: https://docs.yieldyak.com/
[51] "Engineering Error Led to 34 Million USD DeFi Hack, Harvest Finance Says." Accessed: Sep. 1, 2022. [Online]. Available: https://decrypt.co/46445/engineering-error-34-million-defi-hack-harvest-finance
[52] "Axie Infinity." 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://axieinfinity.com/
[53] "MOBOX." 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://www.mobox.io/
[54] "Pulsar Farm." 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://www.pulsar.farm/
[55] Aave. "Open Source DeFi Protocol." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://aave.com/

[56] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra. "An Analysis of Uniswap Markets." Nov. 2020. [Online]. Available: https://cryptoeconomicsystems.pubpub.org/pub/angeris-uniswap-analysis

[57] Ankr. "Ankr Doc." 2022. Accessed: Aug. 15, 2022. [Online]. Available: https://www.ankr.com/ankr-whitepaper-2.0.pdf

[58] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Security Privacy (SP)*, 2017, pp. 375–392.

[59] P. Augustin, R. Chen-Zhang, and D. Shin, "Yield farming," in *Proc. SSRN*, 2022, Art. no. 4063228.

[60] *Avalanche Doc*, Avalanche, Salt Lake City, UT, USA, 2020.

[61] "Balancer." 2021. Accessed: Aug. 15, 2022. [Online]. Available: https://balancer.finance/

[62] Bank of Chain. "Bank of Chain Docs." 2022. Accessed: Sep. 1, 2022. [Online]. Available: https://docs.bankofchain.io/en/

[63] M. Bartoletti, J. H.-y. Chiang, and A. L. Lafuente, "SoK: Lending pools in decentralized finance," in *Proc. Workshop Financ. Cryptography Data Security*, vol. 12676, Dec. 2021, pp. 553–578. [Online]. Available: https://link.springer.com/10.1007/978-3-662-63958-0_40

[64] J. Bertin. "What Is NFT Yield Farming, and How Does it Work?" Jun. 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://www.financebrokerage.com/what-is-nft-yield-farming-and-how-does-it-work/

[65] BNBchain. "BNB Doc." 2022. Accessed: Aug. 15, 2022. [Online]. Available: https://docs.bnbchain.org/docs/bnbIntro/

[66] E. Cecchetti, S. Yao, H. Ni, and A. C. Myers, "Compositional security for reentrant applications," in *Proc. IEEE Symp. Security Privacy*, May 2021, pp. 1249–1267.

[67] "Compound." 2021. Accessed: Aug. 15, 2022. [Online]. Available: https://compound.finance/

[68] S. Cousaert, N. Vadgama, and J. Xu, "Token-based insurance solutions on blockchain," in *Blockchains and the Token Economy: Theory and Practice*. Cham, Switzerland: Springer, Sep. 2022, pp. 237–260. [Online]. Available: https://link.springer.com/10.1007/978-3-030-95108-5_9

[69] S. Cousaert, J. Xu, and T. Matsui, "SoK: Yield aggregators in DeFi," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, May 2022, pp. 1–14. [Online]. Available: https://ieeexplore.ieee.org/document/9805523/

[70] A. Cronje. "YFI. Under Yearn.Finance We Have Released." Jul. 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://medium.com/iearn/yfi-df84573db81

[71] "Curve Finance." 2021. Accessed: Aug. 15, 2022. [Online]. Available: https://curve.fi/

[72] Curve Finance. "Understanding Tokenomics." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://resources.curve.fi/base-features/understanding-tokenomics

[73] A. Das, S. Balzer, J. Hoffmann, F. Pfenning, and I. Santurkar, "Resource-aware session types for digital contracts," in *Proc. IEEE 34th Comput. Security Found. Symp. (CSF)*, 2021, pp. 1–16.

[74] DeFi Llama. "DeFi Leader Board." Accessed: Aug. 15, 2022. [Online]. Available: https://defillama.com/chains

[75] "DeFi Score." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://defiscore.io/

[76] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent dishonesty: front-running attacks on blockchain," in *Proc. Int. Conf. Financ. Cryptography Data Security*, 2019, pp. 170–189.

[77] Ethereum. "Ethereum2 Doc." 2022. Accessed: Sep. 1, 2022. [Online]. Available: https://ethereum.org/en/upgrades/

[78] Fantom. "Fantom Doc." 2018. Accessed: Sep. 1, 2022. [Online]. Available: https://fantom.foundation/research/wp_fantom_v1.6.pdf

[79] Y. Feng, J. Xu, and L. Weymouth, "University blockchain research initiative (UBRI): Boosting blockchain education and research," *IEEE Potentials*, vol. 41, no. 6, pp. 19–25, Nov./Dec. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9935809

[80] L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais, "The decentralized financial crisis," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2020, pp. 1–15. [Online]. Available: https://ieeexplore.ieee.org/document/9150192/

[81] L. Gudgeon, S. Werner, D. Perez, and W. J. Knottenbelt, "DeFi protocols for loanable funds," in *Proc. 2nd ACM Conf. Adv. Financ. Technol.*, New York, NY, USA, Oct. 2020, pp. 92–112. [Online]. Available: https://dl.acm.org/doi/10.1145/3419614.3423254

[82] J. Han, S. Huang, and Z. Zhong, "Trust in DeFi: An empirical study of the decentralized exchange," 2021.

[83] Harvest Finance. "FARM Token Info." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://farm.chainwiki.dev/en/supply

[84] Harvest Finance. "Harvest Finance Yield Farming Strategies." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://farm.chainwiki.dev/en/strategy

[85] Harvest Finance. "Harvest Vault." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://farm.chainwiki.dev/en/education/vault

[86] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019.

[87] Idle Finance. "Distribution—Idle." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://developers.idle.finance/advanced/governance/distribution

[88] Idle Finance. "Idle Finance Documentation." 2021, Accessed: Sep. 1, 2022. [Online]. Available: https://developers.idle.finance/

[89] Jakub. "Yearn Finance and YFI Token Explained." 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://finematics.com/yearn-finance-and-yfi-explained/

[90] H. T. Kao, T. Chitra, R. Chiang, and J. Morrow, "An analysis of the market risk to participants in the compound protocol," in *Proc. 3rd Int. Symp. Found. Appl. Blockchain (FAB)*, 2020, pp. 1–10. [Online]. Available: https://scfab.github.io/2020/FAB2020_p5.pdf

[91] M. Kjaer, M. di Angelo, and G. Salzer, "Empirical evaluation of Makerdao's resilience," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2021, pp. 193–200. [Online]. Available: https://ieeexplore.ieee.org/document/9569811/

[92] R. Leshner. "Expanding Compound Governance." May 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://medium.com/compound-finance/expanding-compound-governance-ce13fcd4fe36

[93] Lido. "Liquidity for Staked Assets." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://lido.fi/

[94] J. Lipstone. "Rari Capital Partners with Saffron Finance." Dec. 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://medium.com/rari-capital/rari-capital-partners-with-saffron-finance-b80c82878c07

[95] S. Mackenzie, "Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial," *Brit. J. Criminol.*, vol. 62, no. 6, pp. 1537–1552, 2022.

[96] H. Markowitz, "Portfolio selection," *J. Finance*, vol. 7, no. 1, pp. 77–91, 1952.

[97] Milkyklim. "Introduction to Yearn." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://docs.yearn.finance/

[98] A. Moin, K. Sekniqi, and E. G. Sirer, "SoK: A classification framework for stablecoin designs," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger, Eds. Cham, Switzerland: Springer Int., 2020, pp. 174–197.

[99] E. Napoletano and B. Curry. "What Is DeFi? Understanding Decentralized Finance." Apr. 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/defi-decentralized-finance/

[100] D. Perez, S. M. Werner, J. Xu, and B. Livshits, "Liquidations: DeFi on a Knife-Edge," in *Proc. Financial Cryptography Data Security*, vol. 12675, 2021, pp. 457–476. [Online]. Available: https://link.springer.com/10.1007/978-3-662-64331-0_24

[101] D. Perez, J. Xu, and B. Livshits, "Revisiting transactional statistics of high-scalability blockchains," in *Proc. ACM Internet Meas. Conf.*, vol. 16, Oct. 2020, pp. 535–550. [Online]. Available: https://dl.acm.org/doi/10.1145/3419394.3423628

[102] I. G. Pernice, S. Henningsen, R. Proskalovich, M. Florian, H. Elendner, and B. Scheuermann, "Monetary stabilization in cryptocurrencies—Design approaches and open questions," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2019, pp. 47–59. [Online]. Available: https://ieeexplore.ieee.org/document/8787560/

[103] Pickle Finance. "Emission Schedule—Pickle Finance Docs." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://docs.pickle.finance/faqs/emissions

[104] M. Platt et al., "The energy footprint of blockchain consensus mechanisms beyond proof-of-work," in *Proc. 21st Int. Conf. Softw. Qual. Rel. Security Companion (QRS-C)*, Dec. 2021, pp. 1135–1144. [Online]. Available: https://ieeexplore.ieee.org/document/9741872/

[105] Polkadot. "Polkadot Doc." 2016. Accessed: Sep. 1, 2022. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf

[106] Polygon. "Polygon Doc." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://polygon.technology/lightpaper-polygon.pdf

[107] PoolTogether. "Home Page." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://pooltogether.com/

[108] A.-D. Popescu, "Transitions and concepts within decentralized finance (Defi) space," *Soc. Sci. Res.*, pp. 40–61, May 2020. [Online]. Available: https://www.researchgate.net/publication/344348838_TRANSITIONS_AND_CONCEPTS_WITHIN_DECENTRALIZED_FINANCE_DEFI_SPACE

[109] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" in *Proc. IEEE Symp. Security Privacy (SP)*, 2022, pp. 198–214.

[110] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," in *Proc. Financial Cryptography Data Security*, vol. 12674, 2021, pp. 3–32. [Online]. Available: https://link.springer.com/10.1007/978-3-662-64322-8_1

[111] "Rari Capital." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://www.rari.capital/index.html

[112] M. Rodler, W. Li, G. O. Karame, and L. Davi, "Sereum: Protecting existing smart contracts against re-entrancy attacks," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2019, pp. 1–9.

[113] K. Saengchote. "Decentralized Lending and Its Users: Insights From Compound." 2022. [Online]. Available: https://ssrn.com/abstract=3925344

[114] K. Saengchote. "Where Do DeFi Stablecoins Go? A Closer Look at What DeFi Composability Really Means." 2022. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3893487

[115] F. Schär, "Decentralized finance: On blockchain- and smart contract-based financial markets," *Fed. Reserve Bank St. Louis Rev.*, vol. 103, no. 2, pp. 153–174, 2021. [Online]. Available: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets?fbclid=IwAR2EJyX0LLThFztaI0kuxOgG6aiXM25mbuiOTl04ZXgvAZjl1NqKxU_fJoc

[116] Solana. "Solana Doc." 2018. Accessed: Sep. 1, 2022. [Online]. Available: https://solana.com/solana-whitepaper.pdf

[117] Sushiswap. "FAQ—xSUSHI." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://docs.sushi.com/faq#xsushi-staking

[118] The European Business Review. "What Is a 'Rug Pull' in Crypto? DeFi Exploits Explained." Jan. 2021. [Online]. Available: https://www.europeanbusinessreview.com/what-is-a-rug-pull-in-crypto-defi-exploits-explained/

[119] P. Tolmach, Y. Li, S.-W. Lin, and Y. Liu. "Formal Analysis of Composable DeFi Protocols." Dec. 2021. [Online]. Available: http://arxiv.org/abs/2103.00540

[120] P. Treleaven, A. Greenwood, H. Pithadia, and J. Xu, "Web 3.0 tokenization and decentralized finance (DeFi)," in *Proc. SSRN*, 2022, Art. no. 4037471.

[121] Uniswap. "Introducing UNI." Sep. 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://uniswap.org/blog/uni/

[122] "Uniswap." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://uniswap.org/

[123] Vesper Finance. "Homepage—Vesper Finance." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://vesper.finance/

[124] Vesper Finance. "Vesper's Tokenomics." Feb. 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://medium.com/vesperfinance/vespers-tokenomics-an-overview-f342ae5b613f

[125] N. Walton, "Yield generation using decentralized financial (DeFi) applications," Ph.D. dissertation, Dept. Comput. Sci., Univ. South Carolina, Columbia, SC, USA, 2022. [Online]. Available: https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1546&context=senior_theses#:∼:text=Decentralized_financial_(DeFi)_applications_are_much_like_a_traditional_bank

[126] Z. Wan, X. Xia, D. Lo, J. Chen, X. Luo, and X. Yang, "Smart contract security: A practitioners' perspective," in *Proc. IEEE/ACM 43rd Int. Conf. Softw. Eng. (ICSE)*, 2021, pp. 1410–1422.

[127] Z. Wang, H. Jin, W. Dai, K.-K. R. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities," *Front. Comput. Sci.*, vol. 15, no. 2, pp. 1–18, 2021.

[128] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt. "SoK: Decentralized Finance (DeFi)." Jan. 2021. [Online]. Available: http://arxiv.org/abs/2101.08778

[129] P. Xia et al., "Trade or trick? Detecting and characterizing scam tokens on uniswap decentralized exchange," in *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 5, 2021, pp. 1–26.

[130] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols," *ACM Comput. Surveys*, to be published. [Online]. Available: https://dl.acm.org/doi/10.1145/3570639

[131] J. Xu and N. Vadgama, "From banks to DeFi: The evolution of the lending market," in *Enabling the Internet of Value: How Blockchain Connects Global Businesses*. Cham, Switzerland: Springer, Apr. 2022, ch. 6, pp. 53–66. [Online]. Available: https://link.springer.com/10.1007/978-3-030-78184-2_6

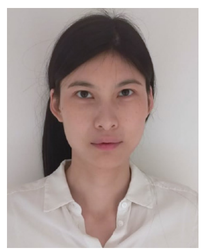
[132] T. A. Xu and J. Xu, "A short survey on business models of decentralized finance (DeFi) protocols," in *Proc. Workshop Financ. Cryptography Data Security*, Feb. 2022, pp. 1–8.

[133] T. A. Xu, J. Xu, and K. Lommers. "DeFi vs TradFi: Valuation Using Multiples and Discounted Cash Flow." Oct. 2022. [Online]. Available: https://arxiv.org/abs/2210.16846

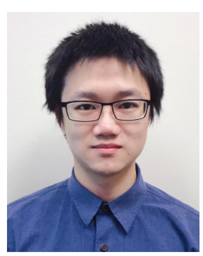
[134] Yearn Finance. "Yearn.Finance." 2021. Accessed: Sep. 1, 2022. [Online]. Available: https://yearn.finance/

[135] L. Zhou, K. Qin, A. Cully, B. Livshits, and A. Gervais, "On the just-in-time discovery of profit-generating transactions in DeFi protocols," in *Proc. IEEE Symp. Security Privacy (SP)*, 2021, pp. 919–936.

[136] ZooKeeper Finance. "ZooKeeper." 2022. Accessed: Nov. 10, 2022. [Online]. Available: https://www.zookeeper.finance/



Jiahua Xu is a Lecturer of Financial Computing and the Programme Director of the M.Sc. Emerging Digital Technologies with the Computer Science Department, University College London (UCL). She is also affiliated to the UCL Centre for Blockchain Technologies and a Founding Member of the U.K. FinTech Academic Network. She has published in Usenix Security, ACM Internet Measurement Conference, Financial Cryptography and Data Security, IEEE International Conference on Distributed Computing Systems, and IEEE International Conference on Blockchain and Cryptocurrency. She has reviewed for Advances in complex systems, computer networks, and transactions on the Web and cities. Her research focuses on blockchain economics and decentralized finance.



Yebo Feng is currently pursuing the Ph.D. degree with the Department of Computer and Information Science, University of Oregon, where he conducts his research in the center for cyber security and privacy. His research interests include network security, blockchain security, and network traffic analysis. He is the recipient of the Best Paper Award of 2019 IEEE CNS, the Gurdeep Pall Graduate Student Fellowship of UO, and the Ripple Research Fellowship. He has served as the reviewer of IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, and ACM Transactions on Knowledge Discovery From Data.