

CeFi vs. DeFi — Comparing Centralized to Decentralized Finance

Kaihua Qin*
kaihua.qin@imperial.ac.uk
Imperial College London

Liyi Zhou*
liyi.zhou@imperial.ac.uk
Imperial College London

Yaroslav Afonin
yaroslav.afonin20@imperial.ac.uk
Imperial College London

Ludovico Lazzaretti
ludovicolazzaretti@gmail.com
Independent

Arthur Gervais
a.gervais@imperial.ac.uk
Imperial College London

Abstract

To non-experts, the traditional Centralized Finance (CeFi) ecosystem may seem obscure, because users are typically not aware of the underlying rules or agreements of financial assets and products. Decentralized Finance (DeFi), however, is making its debut as an ecosystem claiming to offer transparency and control, which are partially attributable to the underlying integrity-protected blockchain, as well as currently higher financial asset yields than CeFi. Yet, the boundaries between CeFi and DeFi may not be always so clear cut.

In this work, we systematically analyze the differences between CeFi and DeFi, covering legal, economic, security, privacy and market manipulation. We provide a structured methodology to differentiate between a CeFi and a DeFi service. Our findings show that certain DeFi assets (such as USDC or USDT stablecoins) do not necessarily classify as DeFi assets, and may endanger the economic security of intertwined DeFi protocols. We conclude this work with the exploration of possible synergies between CeFi and DeFi.

1 Introduction

Centralized finance was originally invented in ancient Mesopotamia, several thousand years ago. Since then, humans have used a wide range of goods and assets as currency (such as cattle, land, or cowrie shells), precious metals (such as gold, which have enjoyed near-universal global cultural acceptance as a store of value), and, more recently, fiat currencies. As such, it has been shown that a currency can either carry intrinsic value (e.g., land) or be given an imputed value (fiat currency). All these known attempts to create an everlasting, stable currency and finance system were based on the premise of a centralized entity, where e.g., a government is backing the financial value of a currency, with a military force at its command. History, however, has shown that currencies can also be valued using an imputed value, that is an assumed value assigned to a currency, which can be unrelated to its intrinsic value, and, e.g., may even be zero.

With the advent of blockchains, and their decentralized, permissionless nature, novel imputed currencies have emerged. One of the blockchain's strongest innovations is the transfer and trade of financial assets without trusted intermediaries [185]. In addition to this, *Decentralized Finance* (DeFi), a new sub-field of blockchain, specializes in advancing financial technologies and services on top of smart contract enabled ledgers [168]. DeFi supports most of the products available in CeFi: asset exchanges, loans, leveraged

trading, decentralized governance voting, stablecoins. The range of products is rapidly expanding, and some of the more complex products, such as options, and derivatives, are rapidly developing as well.

Contrary to the traditional centralized finance¹, DeFi offers three distinctive features: 1. Transparency. In DeFi, a user can inspect the precise rules by which financial assets and products operate. DeFi attempts to avoid private agreements, back-deals and centralization, which are significant limiting factors of CeFi transparency. 2. Control. DeFi offers control to its users by enabling the user to remain the custodian of its assets, i.e., no-one should be able to censor, move or destroy the users' assets, without the users' consent. 3. Accessibility. Anyone with a moderate computer, internet connection and know-how can create and deploy DeFi products, while the blockchain and its distributed network of miners then proceed to effectively operate the DeFi application. Moreover, the financial gain in DeFi also presents a significant contrast to CeFi. In the years 2020 and 2021, DeFi offered higher annual percentage yields (APY) than CeFi: the typical yield of USD in a CeFi bank is about 0.01% [53], while at the time of writing, DeFi offers consistent rates beyond 8% [12]. On the one hand, DeFi enables mirroring traditional financial products, on the other hand, it enables novel financial primitives, such as flash loans and highly-leveraged trading products, that yield exciting new security properties.

In this paper, we aim to compare and contrast systematically the traditional Centralized Finance and Decentralized Finance ecosystems. Firstly, we compare both domains in their technological differences, such as transaction execution order, throughput, privacy, etc. Secondly, we dive into their economic disparities, such as the differences from an interest rate perspective, transaction costs, inflation and possible monetary policies. Finally, we contrast the legal peculiarities, such as regulations around consumer protections, know your customer (KYC) and anti-money laundering (AML) techniques.

In summary, our contributions are the following:

CeFi — DeFi Decision Tree We devise a decision tree which enables the classification of a financial service as CeFi, DeFi, or a hybrid model. We highlight that commonly perceived DeFi

*Both authors contributed equally to the paper.

¹ We prefer to refer to the (currently) traditional finance as CeFi, as centralization is one of the most distinguishing properties, and the term "traditional" might not withstand the test of time.

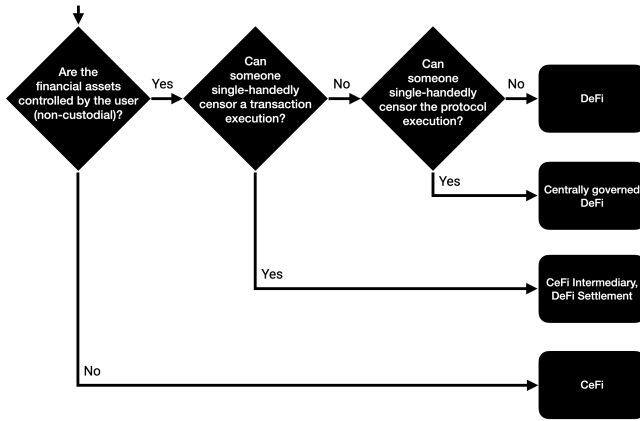


Figure 1: Decision tree to differentiate among DeFi and CeFi.

assets (such as USDC or USDT stablecoins), are in fact centrally governed, allowing a single entity to censor or even destroy cryptocurrency assets. We find that nearly 44M black-listed USDT were destroyed by Tether Operations Limited. We show how this power may lead to significant financial danger for DeFi protocols incorporating these assets.

DeFi Systematization We provide a comprehensive systematization of DeFi, its underlying blockchain architecture and financial services, while highlighting DeFi’s ability to perform a **atomic composability**. We also exposit the various market mechanisms that can be targeted from traditional CeFi as well as novel DeFi market manipulations.

Case Studies We separately provide a case-by-case comparison between CeFi and DeFi focussing on legal, financial services, economics and market manipulations. We conclude the case studies by distilling possible synergies among CeFi and DeFi.

CeFi — DeFi Decision Tree Due to a lack of definition when it comes to DeFi, we have prepared in Figure 1 a possible decision tree that may help classify a financial product or service as CeFi or DeFi. In this tree, the first decisive question is whether the financial assets are held by the user, i.e., whether the user retains control over its own assets. If the user is not in control, does not retain custody nor the ability to transact the assets without a **financial intermediary**, the service is an instance of CeFi. Otherwise, we ask the question whether someone has the capacity to unilaterally censor a transaction execution. Such powerful intermediary points to the existence of a CeFi intermediary, while the asset settlement may still occur in a decentralized, DeFi-compliant manner. Finally, we question whether an entity bears the power to single-handedly stop, or censor the protocol’s execution. If this is the case, we would argue that the DeFi protocol is centrally governed. If this last question can be answered to the negative, the protocol in question would then qualify as a pure DeFi protocol. To the best of our knowledge we are the first to differentiate with three simple and objective questions whether a service is an instance of CeFi or DeFi. Our methodology also highlights that the boundary between CeFi and DeFi is not always as clear-cut as from the first glance.

The paper is organized as follows. Section 2 provides a systematization of DeFi as well as a background on CeFi and applicable properties for the remainder of the paper. Diving into specific case-by-case comparisons, Section 3 focusses on the legal similarities, Section 4 exposes the differences in the financial CeFi and DeFi services, while Section 5 exposes economic and market manipulation analogies. We positively derive possible synergies between DeFi and CeFi in Section 6 and conclude the paper in Section 7.

2 Background

In this section we provide a primer on finance, blockchains, DeFi and its distinguishing properties when considering CeFi.

2.1 What is Finance?

Finance is the process that involves the creation, management, and investment of money [100]. A financial system links those in need of finance for investment (borrowers) with those who have idle funds (depositors). Financial systems play an essential role in the economy since it boosts the economy’s productivity by regulating the supply of money, by ensuring high utilization of existing money supply. Without a financial system, each entity would have to finance themselves, rather than rely on a capital market, and goods would be bartered on spot markets. Such a system would only be able to service a very primitive economy. An effective financial system provides legally compliant, safe, sound, and efficient services to market participants. Financial systems typically consist of the following three components, namely the institution, instrument and market [182]. On a high level, financial institutions issue, buy, and sell financial instruments on financial markets according to the practices and procedures established by laws.

Financial Institutions refer to financial intermediaries, which provide financial services. Traditional financial services include banking, securities, insurance, trusts, funds, etc. Correspondingly, traditional financial institutions include banks, securities companies, insurance companies, trust investment companies, fund management companies, etc. A comprehensive definition of financial institutions is contained in title 31 of the United States Code, including financial auxiliary service providers such as travel agencies, postal services, etc.

Financial Instruments refer to monetary assets. A financial instrument can be a paper document or virtual contract that represents legal agreements involving monetary value. All securities and financial assets (including cryptocurrencies) fall under the broad category of financial instruments.

Financial Markets refer broadly to any marketplace where the trading of financial instruments occurs. Financial markets create liquidity by bringing together sellers and buyers, which helps market participants to agree on a price.

2.2 Blockchains and DeFi

The inception of Bitcoin [148] in 2009 solved the fundamental double-spending problem in a decentralized, electronic setting. For the first time in history, users are able to send and receive online financial assets, without passing through third parties, such as brokers. This very permissionless property of Bitcoin enables users to join and leave the system at their will, without the danger of

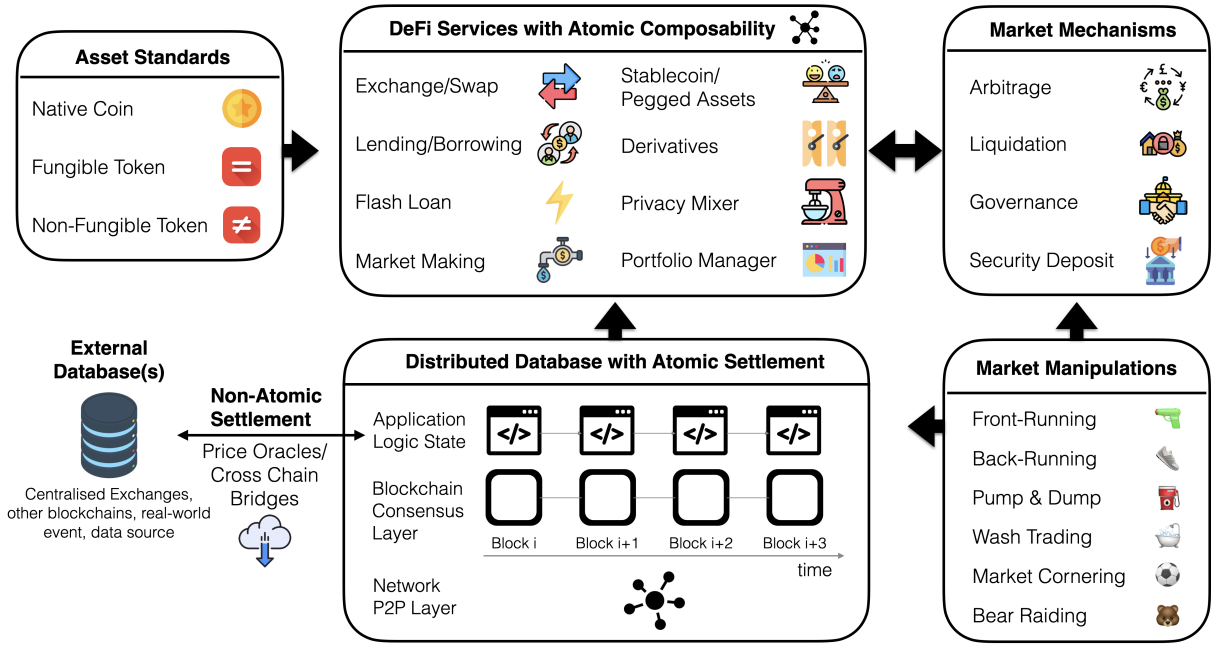


Figure 2: High-level systematization of Decentralized Finance. DeFi builds upon a distributed blockchain database, enabling atomic transaction settlement. Communication with external databases, such as other blockchains, centralized exchanges etc is possible through non-atomic interactions.

assets being frozen by a controlling instance. Crucially, Bitcoin introduced the concept of a time-stamping blockchain, which allows to pin-point the precise time and order at which a transaction should execute. This time-stamping service is critical to the execution of financial assets and allows to unmistakably derive how many financial assets which account holds at which point in time. Bitcoin’s blockchain therefore allows its users to act as the custodian of their own assets, effectively retaining control over their assets. This empowering property creates new opportunities for citizens that are being threatened by malicious governments and irresponsible monetary inflation policies. While Bitcoin supports more complex transactions, fully featured smart contract enabled blockchains truly allow to construct flexible financial products on top of blockchains. With the broader adoption of smart contracts, the concept of Decentralized Finance truly came to fruition, to the point of hosting an economy exceeding 100 Billion USD.

DeFi builds upon the permissionless foundations provided by blockchains. Anyone is free to code and propose a novel financial contract, which anyone is free to interact with, transfer assets to, as well as remove assets from, as long as remaining compliant with the immutable smart contract rules. To provide a higher level intuition of what DeFi is, and can do, we provide the high-level systematization of DeFi in Figure 2.

At its core, a DeFi state transition must be necessarily reflected on its underlying blockchain. For this to happen, a user has to create a transaction, and broadcast this transaction in the public peer-to-peer (P2P) blockchain network. Blockchain miners subsequently pick up the transaction, and depending on the amounts of fees paid by the transaction, the miners may choose to include the transaction

in the blockchain consensus layer. Once a transaction is included in the blockchain, the transaction can be considered to be confirmed, and may be final after a certain time period passed. A confirmed transaction modifies the blockchain and its corresponding DeFi state, by e.g., altering the liquidity provided in an exchange. DeFi builds upon the blockchain’s state machine, whereby various financial services are currently being offered. Those services include lending/borrowing, market-making, stablecoins, pegged tokens, price oracles, privacy services, flash loans, decentralized portfolio managers, insurance and many other [50, 61, 102, 147, 158, 173].

2.3 Properties

In this section we outline the most prevalent DeFi properties.

Public Verifiability: While the DeFi application code may not always be open source, to classify as non-custodial DeFi, its execution and bytecode must be publicly verifiable on a blockchain. Hence, contrary to CeFi, any DeFi user can inspect the DeFi state transitions and verify their orderly execution. Such transparency provides the unprecedented ability to convey trust in the emerging DeFi system.

Custody: Contrary to CeFi, DeFi allows its users to control their assets directly and at any time of the day (there is no need to wait for the bank to open). With such great power, however, also comes great responsibility. Technical risks are mostly absorbed by the users, unless an insurance is underwritten [8, 147]. Therefore, centralized exchanges are very popular for storing cryptocurrency assets [82], which in turn are largely equivalent to traditional custodians.

Privacy: To the best of our knowledge, DeFi is exclusively present on non-privacy preserving smart contract enabled blockchains. As such, these blockchains offer pseudoanonymity, but no real anonymity [160, 165]. A rich literature corpus has already shown how blockchain addresses can be clustered and transaction data can be traced [114, 115, 140, 145, 150, 160, 180]. Given that centralized exchanges with KYC/AML practices are often the only viable route to convert between fiat and cryptocurrency assets, these centralized exchanges have the ability to disclose address ownership to law enforcement.

Atomicity: A blockchain transaction supports sequential actions, which can combine multiple financial operations. This combination can be enforced to be *atomic* — which means that either the transaction executes in its entirety with all its actions, or fails collectively. While this programmable atomicity property is to our knowledge mostly absent from CeFi, (likely costly and slow) legal agreements could enforce atomicity in CeFi as well.

Execution Order Malleability: Through a P2P network, users on permissionless blockchains typically share publicly the transactions that are aimed to be executed. Because of the lack of a persistent centralized entity ordering transaction execution, peers can perform transaction fee bidding contests to steer the transaction execution order. Such order malleability was shown to result in various market manipulation strategies [96, 158, 189, 191], which are widely used on blockchains nowadays [157]. In CeFi, regulatory bodies impose strict rules on financial institutions and services as in how transaction ordering must be enforced [60]. In CeFi this is possible due to the centralized nature of the financial intermediaries.

Transaction Costs: Transaction fees in DeFi and blockchains in general are essential for the prevention of spam. In CeFi, however, financial institutions can opt to offer transaction services at no cost (or are mandated by governments to offer certain services for free [177]) because of the ability to rely on KYC/AML verifications of their clients.

Non-stop Market Hours: It is rare for CeFi markets to operate without downtime. For example, the New York Stock Exchange and the Nasdaq Stock Exchange are the two major trading venues in the United States, and their business hours are Monday to Friday from 9:30 a.m. to 4 p.m. Eastern Time. Due to the non-stop nature of blockchains, most if not all DeFi markets are open 24/7. As a result, DeFi does not have pre- or post-market trading compared to CeFi whereby liquidity on a range of products is typically thin during these periods. Furthermore, system outages at CeFi stock exchanges and CeFi cryptocurrency exchanges have been known to occur due to numbers of users attempting to access the exchanges during times of volatility such as the GameStop short squeeze event, not to mention the intervention by brokerage firms to restrict their respective customer's purchase and sale of certain equity products due to liquidity and solvency concerns [41, 44].

Anonymous Development and Deployment: Many DeFi projects are developed and maintained by anonymous teams², even the Bitcoin creator remains to date anonymous. Once deployed, the miners implicitly operate the DeFi smart contracts. Anonymous DeFi projects can function without a front-end, requiring users to interact with the smart contract directly. Alternatively, the front-end website can be served through a distributed storage service, such as IPFS.

3 Case by Case — Legal

In the following we focus on the legal aspects of CeFi and DeFi.

3.1 On-boarding and Continuous Compliance

When opening an account with a financial institution in CeFi, in most countries, it means that the user needs to visit a nearby branch, or online portal and follow the on-boarding steps. CeFi heavily relies on KYC verifications, which are required by regulations [159]. KYC typically involves the verification of the identity, through an ID, passport or a driver's license. Moreover, the user is usually required to provide a proof of address or residency. Depending on local regulations, and the user's intent, the user may also be required to answer questionnaires to clarify its financial background (i.e., whether the user is knowledgeable about the financial risks of different asset classes). Finally, depending on the user's intent, the financial institution may also require a proof of accredited investor, for example showing that the user's net worth exceed the respective jurisdiction's threshold to admit them for accessing certain sophisticated services, or requesting formal classification as a non-retail participant which entails losing their rights to complain to the Financial Ombudsman (e.g. in the UK) or other financial regulator [36]. Depending on the user's background, intentions and the financial institution, this KYC process may take from a few hours to several weeks. As such, compliance checks are especially challenging in a worldwide setting, with many different passport formats and qualities. Therefore, dedicated companies are nowadays offering on-boarding services [25]. While KYC is certainly very helpful in combating illegal activities, compliance checks significantly increase the bureaucratic overhead and associated costs when offering financial services in CeFi.

Besides KYC, AML verifications in CeFi are typically an ongoing effort to verify the source, destination and purpose of asset transmissions by financial institutions [146, 170]. AML's purpose is to combat money laundering, as in to differentiate between benign and malicious sources of funds and, in most jurisdictions, a senior official at the financial institution is required to act as the Money Laundering Reporting Officer or similar nominated role [36]. **With the advent of DeFi, and blockchain transactions in general, CeFi financial institutions are known to thoroughly investigate funds with a DeFi provenance** [14]. Yet, it is technically much simpler to trace DeFi funds than CeFi assets due to the open and transparent nature of blockchains. Therefore, we expect CeFi institutions to further accept DeFi assets, for which a user is able to justify the source of funds. Note that some CeFi institutions simply avoid accepting DeFi or blockchains assets due to the increased compliance

²Such as Harvest Finance on Ethereum and Pancakeswap on Binance Smart Chain.

overhead and costs which are at times (depending on jurisdictions) onerous and costly for traditional CeFi participants.

Because DeFi assets and transactions are typically traceable through investigating the publicly accessible blockchain, KYC/AML-enabled CeFi exchanges, which provide fiat and cryptocurrency assets trading pairs, can offer law enforcement helpful identity information in combating money laundering [2]. However, if a user solely operates within DeFi, without ever crossing the boundary into CeFi, it is technically possible to entirely avoid KYC. Moving non-KYC'd assets to CeFi, may however prove to be challenging from a compliance perspective.

Insight 1: Linking DeFi assets from CeFi

The on-boarding process in DeFi typically requires a CeFi intermediary, and hence discloses the blockchain addresses of the respective users. DeFi's transparency would then allow to trace the coins provenance.

3.2 Asset Fungibility in CeFi and DeFi

The Financial Action Task Force (FATF) is an intergovernmental organization with the aim to develop policies to combat money laundering and the financing of terrorism (CFT) [23]. The FATF recommendations are increasingly being accepted by major jurisdictions, also affecting DeFi. For instance, the FATF introduced terms such as virtual asset service provider (VASP), and the *travel rule*. VASPs are e.g., entities which hold assets on behalf of users, such as custodians. However, as of now, it is unclear whether an individual who deploys a DeFi protocol would be classified as a VASP [55]. The FATF rules may render a software engineer liable for developing a DeFi application, even if this developer does not retain any control over the deployed application, nor is involved in the launch or post-launch activities [24]. The travel rule requires financial institutions (in particular VASPs) to notify the receiving financial institutions about a cryptocurrency transactions along with its identifying information [1, 19, 39].

Censoring (Temporarily) Transactions In Figure 1 we provide a decision tree on how to differentiate between CeFi and DeFi services, whereas this tree is substantially influenced by the legal peculiarities at stake. One critical differentiation therein is whether someone has the option to censor a transaction, or an entire protocol execution. Regulators, e.g., in Switzerland, are known to impose AML rules on non-custodial providers which have the ability to intervene, i.e., censor, a transaction [48]. In practice, there may appear many services capable of first temporarily censoring transactions, as well as services that may indefinitely block the execution of a particular transaction.

Miners in Bitcoin for instance, are certainly empowered to not include a transaction in the blockchain, and hence have the ability to temporarily censor a transaction execution. In Lightning [156] for instance, nodes may simply refuse to provide service for a particular transaction, forcing the user to either chose another off-chain payment path, or return to the on-chain layer through a regular Bitcoin transaction. Alternative off-chain technologies, such as commit-chains, which are possibly operating a single centralized,

```

1 function transfer(address _to, uint _value) public
  whenNotPaused {
2   require(!isBlackListed[msg.sender]);
3   if (deprecated) {
4     return UpgradedStandardToken(upgradedAddress).
      transferByLegacy(msg.sender, _to, _value);
5   } else {
6     return super.transfer(_to, _value);
7   }
8 }
9 function addBlackList (address _evilUser) public
  onlyOwner {
10  isBlackListed[_evilUser] = true;
11  AddedBlackList(_evilUser);
12 }
13 function destroyBlackFunds (address _blackListedUser)
  public onlyOwner {
14  require(isBlackListed[_blackListedUser]);
15  uint dirtyFunds = balanceOf(_blackListedUser);
16  balances[_blackListedUser] = 0;
17  _totalSupply -= dirtyFunds;
18  DestroyedBlackFunds(_blackListedUser, dirtyFunds);
19 }

```

Listing 1: USDT code blacklist functionality.

but non-custodial server, may have the ability to censor transactions, and may hence also require to meet KYC/AML requirements.

Insight 2: Censoring transactions and KYC/AML requirements

If an entity is able to single-handedly censor or intervene in a financial transaction, this entity may become liable to KYC/AML/CFT requirements, even if the entity is not an asset custodian.

Blacklists, Fungibility and the Destruction Assets Once a financial service provider is subject to KYC/AML requirements, the financial enforcement authorities of the respective legislation may request and require the ability to freeze and confiscate financial assets. This requirement, however, fundamentally contradicts with the non-custodial property and vision, on which Bitcoin and its many permissionless follow-up variants are built upon.

For instance, the stablecoins USDT and USDC have a built-in smart contract functionality to add specific blockchain addresses on a blacklist (cf. Listing 1). Once a blockchain address is added to this blacklist, this address cannot send USDT or USDC coins or tokens any longer (while USDT can still be received). Moreover, the company behind USDT retains the capability to entirely zero the balance of a blacklisted address. While we have not found a public statement, we believe that the blacklist functionality was implemented due to a regulatory requirement. By collecting the entirety of the Ethereum blockchain events since USDT's and USDC's inception, we observe that 449 accounts are blacklisted by the USDT smart contract (8 of these accounts were removed from the blacklist) at the time of writing. Alarmingly, a total of over 43.97M USDT were destroyed. The USDC contract features 8 blacklisted accounts. We find no overlap between the USDT and USDC blacklist.

DeFi "Bank Run" The ability to blacklist, or even destroy cryptocurrency assets by a central body certainly contradicts DeFi's non-custodial vision. Technically, such feature moreover endangers the intertwined DeFi ecosystem as we show in the following.

DeFi is heavily reliant on liquidity pools which are governed by smart contracts accepting a variety of different tokens. A user that deposits tokens in a liquidity pool, receives in return a liquidity provider (LP) token, which accounts for the user’s share in the pool.

Exchanges as well as lending platforms, such as Aave [61] and Curve [13], advertise various pools that contain USDT tokens. If the company behind USDT would choose to block the address of the smart contract liquidity pool containing USDT, all users of such pools are affected, irrespective of whether their USDT are benign or illicit assets. An adversary with illicit USDT would moreover be incentivised to deposit its illegally acquired USDT within such liquidity pools, as blacklisting the adversary’s blockchain addresses wouldn’t yield any effects thereafter.

If a Curve liquidity pool containing USDT is blacklisted by the USDT emitter, all users of this pool would exit the pools through the other (fungible) pool assets. To that end, the user will return to the smart contract its LP tokens, and demand the non-blacklisted assets. Contrary to a bank run in CeFi, the smart contract will not seize operation, but provide the user a possibly significantly worse exchange rate for the LP tokens. That is, because the pricing formula of liquidity pools typically penalizes users that move the pool away from its assets equilibrium. Worryingly, such a DeFi “bank run” would cause in particular losses to those that act last.

Insight 3: “Bank Run” in DeFi

If an entity can single-handedly blacklist, censor, or destroy specific cryptocurrency assets, this asset poses a danger to smart contracts relying on its fungible property, and can trigger a DeFi “bank run”. Contrary to a CeFi bank run, a DeFi bank run will return assets to the user, however, at a much worse exchange rate. Smart contract liquidity pools are currently not adept to fine-grained AML that CeFi relies upon.

4 Case by Case — Services

In the following we compare objectively various financial services and highlight how DeFi and CeFi differ respectively. We outline the service architecture of CeFi and DeFi in Figure 3. Notably, oracles and stablecoins (specifically, stablecoins with the reserve of pegged asset mechanism) interconnect CeFi and DeFi.

DeFi protocols frequently rely on CeFi data to function. Stablecoins, for example, typically require the USD-to-cryptocurrency conversion rate to maintain the peg. However, blockchains do not natively support access to off-chain data. Oracles are a third-party intermediary service that aims to address this issue by feeding external data (including CeFi data) into DeFi [62, 70, 79, 83, 139, 161, 173, 187, 188]. Due to the high cost of writing data to the chain, the frequency of an oracle’s updates is typically several orders of magnitude lower than the frequency of CeFi price changes.

4.1 CeFi vs. DeFi Exchanges

An exchange is a marketplace where financial instruments are traded. Historically, this can occur on a physical location where traders meet to conduct business, such as NYSE. In the last decades, trading has transitioned to centralized electronic exchanges. A

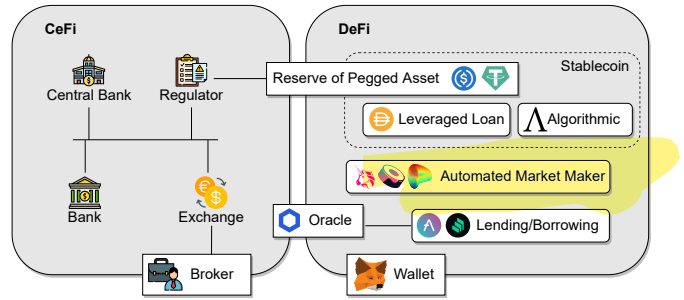


Figure 3: High-level service architecture of CeFi and DeFi.

modern electronic exchange typically consists of three components: (i) a price discovery mechanism, (ii) an algorithmic trade matching engine, and (iii) a trade clearing system. The degree of decentralization of an electronic exchange depends on whether each of these three components is decentralized. The literature and practitioners community features various exchange designs based on blockchain architectures (DEX) [117, 178, 184], trusted execution environments (TEE) [80, 91, 93, 137, 138] and multi-party computation (MPC) [126, 127] (cf. Table 1).

Exchanges can also be categorized based on the traded asset pairs. Decentralized, blockchain-based clearing systems, typically only support cryptocurrency assets, or tokens, and stablecoins representing fiat currencies. Contrary to DeFi, in centralized CeFi exchanges (CEX), there exists standalone custodians, and the exchange is segregated from the custodian for safety reasons, with custodians typically being large banks [107, 131]. CEX can support the flexible trading of both fiat and cryptocurrencies.

Financial Instrument Listing A CEX usually has specific asset listing requirements [149, 155], including the provision of financial auditing and earning reports, minimum working capital statements, etc. However, for centralized cryptocurrency exchanges, to our knowledge, there exists no binding legal requirement for asset listings. Therefore, centralized cryptocurrency exchanges may accept, or refuse the listing of financial instruments due to subjective or political reasons. One advantage of a DEX is that the exchange governance may be achieved in a decentralized manner, such that the listing of assets may be transparent. For instance, the only requirement for a listing on Uniswap is that the financial instrument meets the ERC20 standard [20].

High-frequency Trading (HFT) HFT refers to automated trading strategies that aim to profit from short-term market fluctuations. Previous research has revealed a variety of CEX HFT strategies and their economic impact, including arbitrage, news-based trading, algorithmic market making, etc. [63, 69, 84, 141]. Although DEX are fundamentally different from CEX in terms of their technical design, traditional HFT strategies remain similar in DEX [96, 157].

In the following, we focus on one of the most basic HFT strategies, namely two-point arbitrage, in which a trader purchases a financial instrument in one market and then sells the same instrument at a higher price in a different market. Two-point arbitrage eliminates short-term price discrepancies between two markets, resulting in an increased market efficiency. Other types of HFT strategies are

Table 1: Comparison of different types of CeFi and DeFi exchanges.

	Centralized (CEX)		Hybrid	Decentralized (DEX)		
Exchange Name	NASDAQ [38]	Coinbase [5]	IDEX [129]	0x [184]	Tesseract [81]	Uniswap [178]
Currencies	USD	Fiat + Crypto	Crypto	Crypto	-	Crypto
Governance	Centralized	Centralized	Centralized	DAO	Centralized	DAO + smart contract
Price discovery mechanism	Centralized	Centralized	Centralized	Decentralized	TEE	Smart contract
Trade matching engine	Centralized	Centralized	Centralized	Decentralized	TEE	Smart contract
Clearing system	Centralized	Centralized	Blockchain	Blockchain	Blockchain	Blockchain
Can manipulate transaction order?	Regulated	Regulated	Yes	Yes	No	Yes (Miners)
Can reject valid transaction?	Regulated	Regulated	Yes	Yes	No	Yes (Miners)

similar to two-point arbitrage in terms of execution, despite being different in their execution methodologies.

Arbitrage Execution HFT strategies are known to be fiercely competitive [63, 72, 76, 85, 116]. In the case of a two-point arbitrage opportunity, the arbitrageur with the fastest execution speed on both exchanges remains profitable in expectation.

In CEX and hybrid exchanges, arbitrageurs typically interact directly with a centralized service provider (e.g., the exchange itself) to obtain the most recent market state to execute their transactions. Arbitrageurs invest in high performance computing resources and optimize their source code and hardware to achieve lower latencies [92]. Arbitrageurs are known to even physically relocate servers closer to the corresponding exchange to further reduce network layer latency. The recent advent of low-orbit satellite internet service [17], was shown to further reduce the global internet latency by as much as 50% [111], which we therefore expect to be a prime communication medium for HFT.

Messages in blockchain-based DEX by design propagate on the public peer-to-peer (P2P) network. Therefore, at the transaction creation time, it is not known which node, or miner, will execute the transaction. To gain a competitive advantage, an arbitrageur must aim to reduce its latency to all major miners and mining pools. To that end, arbitrageurs can run multiple blockchain nodes in different physical locations around the world, as well as maximize the number of connections for each node to decrease transaction reception latency [106] and transaction broadcast speeds [191].

Arbitrage Risks An arbitrage should ideally execute atomically to reduce the risks of price fluctuations. In practice, arbitrage on centralized and hybrid exchanges is unavoidably subject to market price fluctuations, unless the arbitrageurs are colluding with the exchanges to guarantee execution atomicity.

Arbitrage between two decentralized exchanges on the same blockchain can be considered risk-free, when ignoring transaction fees. This is because traders can use the blockchain atomicity feature to create a smart contract that executes the arbitrage, and reverts if the arbitrage does not yield a profit. If, however, an arbitrage attempt reverts, the trader is still liable to pay the transaction fees. It should be noted that the atomicity property is only preserved for arbitrage among different DEX on the same blockchain. If the arbitrage involves two DEX on different blockchains, the arbitrage risk can be considered similar to that of a CEX and hybrid exchange.

4.2 DeFi vs. CeFi Lending/Borrowing

Lending and borrowing are ubiquitous services in CeFi. Credit, offered by a lender to a borrower, is one of the most common forms of lending [9]. Credit fundamentally enables a borrower to purchase goods or services while effectively paying later. Once a loan is granted, the borrower starts to accrue interest at the borrowing rate that both parties agree on in advance. When the loan is due, the borrower is required to repay the loan plus the accrued interests. The lender bears the risk that a borrower may fail to repay a loan on time (i.e., the borrower defaults on the debt). To mitigate such risk, a lender, for example, a bank, typically decides whether to grant a loan to a borrower based on the creditworthiness of this borrower, or mitigates this risk through taking collateral - shares, assets, or other forms of recourse to assets with tangible value. Creditworthiness is a measurement or estimate of the repaying capability of a borrower [10]. It is generally calculated from, for example, the repayment history and earning income, if it is a personal loan. In CeFi, both lenders and borrowers can be individuals, public or private groups, or financial institutions.

On the contrary, in DeFi, the lack of a creditworthiness system and enforcement tools on defaults leads to the necessity of over-collateralization in most lending and borrowing protocols (e.g., Aave [61], Compound [102]). Over-collateralization means that a borrower is required to provide collateral that is superior to the outstanding debts in value. Such systems are also widespread in CeFi and are known as margin lending or repo-lending [128]. The most prevalent form of lending and borrowing in DeFi happens in the so-called lending pools. A lending pool is in essence a smart contract that orchestrates lender and borrower assets, as well as other essential actors (e.g., liquidators and price oracles). Typically, a lender makes cryptocurrencies available for borrowing by depositing them into a lending pool. A borrower hence collateralizes into and borrows from the lending pool. Note that borrowers also automatically act as lenders when the lending pool lends out the collateral from borrowers. Assets deposited by users in lending pools are not protected by traditional CeFi regulations such as bank deposit protection which protects a banking institution's customer deposit account up to a certain threshold of fiat currency.

To maintain the over-collateralization status of all the borrowing positions, lending pools need to fetch the prices of cryptocurrencies from price oracles. Once a borrowing position has insufficient collateral to secure its debts, liquidators are allowed to secure this position through liquidations. Liquidation is the process of a liquidator repaying outstanding debts of a position and, in return, receiving

the collateral of the position at a discounted price. At the time of writing, there are two dominant DeFi liquidation mechanisms. One is the fixed spread liquidation, which can be completed in one blockchain transaction [61], while the other one is based on auctions that require interactions within multiple transactions [103].

Under-collateralized borrowing still exists in DeFi (e.g., Alpha Homora [27]), while being implemented in a restricted manner. A borrower is allowed to borrow assets exceeding the collateral in value, however, the loan remains in control of the lending pool and can only be put in restricted usages (normally through the smart contracts deployed upfront by the lending pool). For example, the lending pool can deposit the borrowed funds into a profit-generating platform (e.g., Curve [13]) on behalf of the borrower.

Flash Loans A novel lending mechanism, which only exists in DeFi, are flash loans [158]. A flash loan is initiated and repaid within a single, atomic blockchain transaction, in which a borrower *B* performs the following three actions:

- (1) *B* requests assets from a flash loan lending pool.
- (2) *B* is free to use the borrowed assets arbitrarily.
- (3) *B* repays the flash loan plus interests to the lending pool.

The transaction atomicity property (cf. Section 2.3) ensures that, if the borrower cannot repay the flash loan by the end of the transaction, the on-chain state remains unmodified (i.e., as if no flash loan was granted) [65, 158]. Therefore, although the borrowers do not provide collateral for the loan, the lenders can be sure, that the borrowers cannot default on their debt.

Flash loans are widely applied in DeFi arbitrages and liquidations, as they allow to eliminate the monetary risks of holding upfront assets [158, 183]. Flash loans, however, also facilitate DeFi attacks that have caused a total loss of over 100M USD to victims in the year 2020 alone [15, 28, 33, 158]. Despite the fact that flash loans are not the root vulnerability of these DeFi attacks, they do give adversaries instant access to billions of USD, costing only a minor upfront cost (i.e., the blockchain transaction fees). To our knowledge such instantaneous loans have no counterpart in CeFi.

Insight 4: Flash loans facilitate DeFi attacks

Flash loans are typically not the cause, but facilitate DeFi attacks by granting adversaries instant access to billions of USD of capital. In essence these loans therefore democratize access to capital, lowering the barriers of entry to a market which traditionally is exclusive to few in CeFi.

Risk Free Rate of Return The risk-free rate of return is a crucial concept in CeFi, referring to the theoretical rate of return that an investor expects to earn from a risk-free investment [43]. The notion is critical to a functioning financial system and underpins valuation of almost every major financial product, bank deposit, loans, government/corporate bond, and the valuation of stocks. Although there exists no absolutely risk-free investment opportunity in practice, the interest rate of some investments with a negligible risk is commonly considered as the risk-free rate. For instance, U.S. government bonds are generally used as risk-free rates because it is unlikely that the U.S. government will default on its debt [58]. It is unclear whether a risk-free investment opportunity exists in

DeFi, especially when we consider the various risks imposed by the underlying smart contracts and blockchain consensus (e.g., potential smart contract program bugs). We, however, observe that several DeFi protocols may yield revenue in a risk-free manner, if we only consider the high-level economic designs while ignoring the risks from the underlying layers³. For example, MakerDAO, the organization behind the stablecoin DAI (cf. Section 4.3), offers interests to the investors who deposit DAI into a smart contract at the so-called DAI saving rate (DSR). DSR is a fixed non-negative interest rate, which is convertible through a governance process. Similarly, the interests generated from the aforementioned lending platforms (e.g., Aave, Compound) are generally considered low-risk. The lending interest rate is typically determined algorithmically through the supply and demand of the lending pool, which is hence more variable than the DAI saving rate. At the time of writing, MakerDAO offers a DAI saving rate of 0.01%. The estimated annual percentage yield (APY) of DAI on Compound and Aave is 3.18% and 5.65%, respectively. As a comparison, the U.S. 10-year government bond has a 1.623% yield [51].

4.3 CeFi vs. DeFi Stablecoins

Cryptocurrencies are notoriously known for their price volatility which appeals to speculators. However, conservative traders may prefer holding assets that are less volatile. Stablecoins are hence designed to satisfy such demand and offer better price stability. The price of a stablecoin is typically pegged to a fiat currency (e.g., USD), which is less volatile than most cryptocurrencies. Following related work [144], we proceed to summarize the dominating DeFi stablecoin mechanisms.

Reserve of Pegged Asset One method to create a stablecoin is to collateralize the asset that the stablecoin should be pegged to (e.g., USD) in a reserve to back the value of the minted stablecoin. Such mechanism commonly requires a centralized and trusted authority to manage the collateralized assets. This authority is permitted to mint the stablecoin, while any entity is allowed to burn the stablecoin in exchange for the collateral at the pegged price (e.g., burning one unit of USD stablecoin allows to redeem \$1). When the stablecoin price declines below the pegged price, arbitrageurs are incentivized to purchase the stablecoin to redeem the collateral, which in return supports the stablecoin price. Conversely, when the price rises above the peg, more stablecoins are minted and hence the expanded supply may depreciate its price. In this way, such mechanism aims to stabilize the minted stablecoin value to the pegged asset. With an accumulated volume of over 49B USD, USDT and USDC are the most circulated stablecoins following the above mechanism. According to our CeFi-DeFi decision tree (cf. Figure 1), the stablecoins adopting the asset reserve mechanism are non-custodial. Second, a stablecoin transaction cannot be censored by a third party. However, given the blacklist functionality (cf. Section 3), the stablecoin issuing authority can censor the protocol

³In CeFi, the risk free rate of return is typically defined regionally. Local currency investors use the central bank bond yields of their respective countries to estimate their individual risk-free rate. For example, an investor based in Brazil whose P&L currency is BRL will rely on the interest rate of Brazilian government bonds for estimating premium of their investments over their BRL-denominated risk-free rate. In such context, we deem a DeFi investment opportunity risk-free, when it is programmatically guaranteed to offer a positive return in the same invested cryptocurrency.

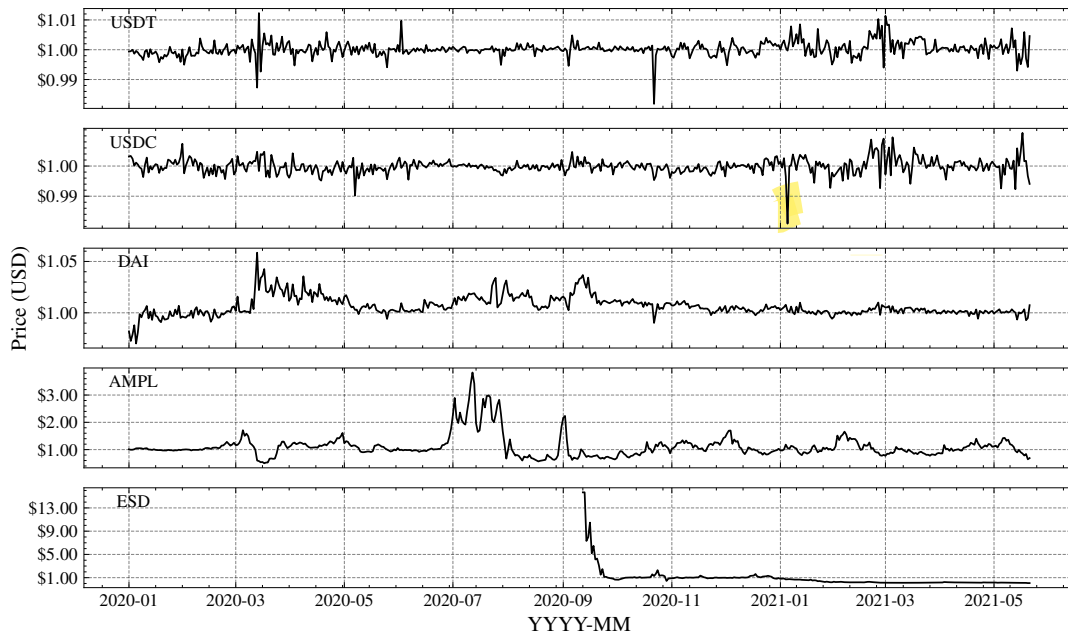


Figure 4: Prices of USD stablecoins, USDT, USDC, DAI, AMPL, and ESD from January, 2020 to May, 2021. We crawl the price data from <https://www.coingecko.com/>.

execution. Therefore, such stablecoins are instances of centrally governed DeFi. Moreover, the main drawback of this stablecoin mechanism is the necessity of a trusted authority. The authority’s ability to blacklist addresses may help with regulatory compliance (cf. Section 3) but harms the decentralization of DeFi.

Leveraged Loans The mechanism of leveraged loans also relies on collateral to secure the value of a stablecoin. Instead of collateralizing fiat assets, which demands a centralized authority, the leveraged loan mechanism accepts cryptocurrencies (e.g., ETH) as collateral. DAI is the most prominent stablecoin that follows this mechanism. To mint DAI, a user creates a Collateralized Debt Position (CDP) by locking cryptocurrencies into a smart contract. In the following, we refer to this user as the CDP owner. The CDP owner is allowed to mint DAI from the CDP, where the minted DAI becomes the owner’s debt. A CDP is required to be 1.5× over-collateralized, i.e., the value of the collateral represents at least 150% of the debt. Otherwise, the CDP would become available for liquidations (cf. Section 4.2). When compared to the asset reserve mechanism, the over-collateralization design makes the leveraged loan mechanism less capital efficient. For instance, a collateral of 150B USD can mint at most 100B USD of leveraged loan stablecoins.

Algorithmic Supply Adjustments Instead of collateralizing fiat or other cryptocurrencies, an algorithmic stablecoin attempts to maintain the stablecoin price autonomously. Specifically, the algorithmic supply adjustment mechanism adjusts the supply of the stablecoin in response to price fluctuations. The main idea of an algorithmic stablecoin is that the adjustment of the supply can effectively drive the price of the stablecoin towards the desired target. Typically, the adjustment algorithm is encoded within a

smart contract. Therefore, the supply adjustment can be processed autonomously without a central entity.

In Figure 4, we present the prices of five stablecoins. USDC and USDT are reserve-based, while DAI relies on leveraged loans. AMPL and ESD, are algorithmic stablecoins. We find that the reserve mechanism appears the most stable among the dominating stablecoin solutions, with a price fluctuation range between \$0.99 and \$1.01 since January 2020. DAI is less stable than USDC and USDT, but shows increasing stability since January 2021. To our surprise, the mechanisms of algorithmic supply adjustments appear ineffective in stabilizing the price. AMPL fluctuates between \$0.50 and \$3.83. ESD presents a downtrend deviating from the \$1 target price, closing at \$0.1 at the time of writing.

Although the term stablecoin emerged in DeFi, CeFi aims for decades to stabilize currency prices [37]. The Hong Kong dollar (HKD), for example, is pegged to the US dollar [57], permitted to be traded at a tight interval between 7.75 and 7.85 USD [59]. Within this price range, the Hong Kong Monetary Authority intervenes through buying or selling the currency.

Insight 5: Algorithmic stablecoins are less stable in practice

Given empirical data, we observe that stablecoins based on the mechanism of algorithmic supply adjustments offer less stability than reserve and loan based stablecoin models.

5 Case by Case — Economics & Manipulation

Next we dive into the economic and market manipulation aspects of CeFi and DeFi.

5.1 CeFi vs. DeFi Inflation

Inflation is defined as the devaluation of an existing currency supply, through the addition of more supply [120]. While inflation is the loss of purchasing power of a currency, the relationship between supply and inflation may not always manifest itself directly — sometimes money supply increases, but does not cause inflation [86].

In CeFi, central banks retain the authority to create their respective fiat currency, and inflation is typically measured against the value of “representative basket of consumer goods”, or a consumer price index (CPI) [119]. The official policy goal of central banks in developed markets is to keep the inflation at or around 2.0% [75, 152]. Inflation in developed countries in recent decades has rarely diverged from central bank official targets. While there have been several notable instances of high inflation or hyperinflation historically (Germany 1923, USA in 1970s, certain emerging market countries like Argentina, Venezuela, Zimbabwe), in recent decades official inflation figures in the USA, Europe, and other major economies have rarely been above 3.0%.

However, despite the positive picture painted by central banks, many market participants doubt whether the basket of consumer goods is representative. Various social group baskets can vary dramatically, making the 2.0% headline inflation rate irrelevant in their context. In the USA, in recent decades the richest 1% of the population have seen their incomes rise at a much faster pace than the bottom 50%, who have seen little inflation-adjusted increase. For example, as of mid-April 2021, the year-to-date increase in price of Lumber is circa 40% [176], the main cost component in house construction, while the CPI in the USA is at 2.6% [154]. This, and similar increases in prices of many goods, have cast doubts whether the official inflation figures really measure inflation accurately.

Central banks have learned to print money without causing broad CPI-inflation - rather than giving money directly to consumers like in 1920s Germany, money is now effectively distributed to asset holders — so they can purchase more risky assets, driving their prices up. This, in turn, supports the economy by ensuring people with capital continue investing and creating jobs. The flipside is that people who do not own assets, see the value of their savings inflated away. Bitcoin’s fixed supply protects from the risk of the currency being printed into zero (like Venezuela or Zimbabwe did), however, whether having a fixed supply is advantageous is not yet clear. Fiat currencies also used to have a fixed supply system similar to that of Bitcoin - until 1974 when the gold standard was scrapped, and each dollar no longer had to be backed by a specific quantity of gold [97]. The standard was scrapped because it constrained countries’ ability to support economic activity.

Some cryptocurrencies have variable asset supply. Bitcoin eventually is likely to run into the issue where supply has a hard cap — while the economic activity it has to support does not have a cap — leading to a shortage of currency. Related work suggests that Bitcoin, or blockchains in general, without a block reward, and hence without inflation, might be prone to security instabilities [87]. Whether Bitcoin and other cryptocurrencies end up suffering from high income inequality from the inflation built into the fiat system is yet to be seen — there is no conclusive track record as of yet to suggest cryptocurrencies solve this problem. Many people have come to see cryptocurrencies as a way to liberate themselves from

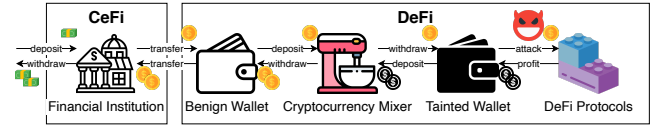


Figure 5: Example of money laundering with a DeFi attack.

the influence of central banks [169]. Ethereum, however, bears an inflation rate of about 4%. This metric is most directly comparable to measures of monetary mass, such as M1 [101], which, by contrast, increased by circa 250 percent in 2020, due to money printing by the Federal Reserve.

5.2 Mixer and DeFi Money Laundering

To our knowledge, for blockchains without native privacy preserving functionality, address linkability (i.e., the process of linking n blockchain addresses to the same entity) can only be broken with a mixing service. A mixer allows users to shuffle their coins with the coins of other users [68, 104, 118, 142, 166]. This may appear similar to CeFi’s traditional money laundering techniques, in which the money launderer mixes tainted, or “dirty”, and “clean” money. The literature contains a number of proposals for mixer services that can be either centralized or governed by smart contracts. Because of DeFi’s traceability, the source and amounts of both benign and illicit assets, as well as the anonymity set sizes, the source code and the mixing cost, are all public. Ironically, from a technical standpoint, this transparency greatly reduces the risk of the money launderer. Worryingly, mixer services have begun to reward their users for participation, providing an economic reason for DeFi users to provide untainted assets to help money laundering [49, 132].

5.3 CeFi vs. DeFi Security and Privacy

DeFi attacks can be broadly classified into five attack types: (i) network layer; (ii) consensus layer; (iii) financial institution; (iv) smart contract code; and (v) DeFi protocol and composability attacks. Attacks of type (iii) and (iv) use a mixer to perform money laundering (cf. Figure 5). In the following sections, we outline each attack type.

Network Layer Attacks Previous research has revealed how an adversary can partition the blockchain P2P network without monopolizing the victim’s connections. This allows an adversary to control the victim node’s view of the blockchain activity. Eclipse attacks can occur at the infrastructure layer (such as BGP hijacking [73, 167]) or during blockchain message propagation [106]. Other types of common network attacks, such as DDoS [163], MitM[98], and wireless network attacks [151], are also possible in DeFi. An attacker could, for example, use the evil twin attack [130] to impersonate a wireless access point to trick users into connecting to bogus DeFi smart contracts. For further information, we refer the interested reader to previous literature [162].

Consensus Layer Attacks Consensus attacks such as double spending [124, 125] and selfish mining [99, 108, 164] endanger the stability and integrity of the DeFi settlement layer. For more details, we refer the reader to extensive previous studies [105, 134, 135].

Financial Institution Attacks Ideally and to maintain its decentralized vision (cf. Figure 1), DeFi should solely rely on smart contracts ignoring third party intermediaries. However, in practice, DeFi is still heavily reliant on centralized intermediaries such as wallet providers (MetaMask [34], Coinbase wallet [7], etc.), blockchain API providers (Infura [30]), mining pools (SparkPool [47], Ethermine [22], etc.) and oracles [173]. Aside the risks of downtime and code vulnerabilities, it is important to note that these intermediaries are typically run by physical businesses that may be forced to close due to local laws and regulations [3].

Smart Contract Code Attacks Smart contract vulnerabilities in DeFi have already caused at least 128M USD of losses to users (cf. Table 3) [16, 29, 40, 42, 52]. Common vulnerability patterns include integer overflow, reentrancy, timestamp dependencies, etc [74]. For example, in April 2020, the lending platform “Lendf.Me” suffered a re-entry attack, resulting in the loss of 25M USD in funds [29]. To our knowledge, the most significant smart contract code vulnerability resulted in an adversarial profit of 57M USD on the “Uranium Finance” platform in April 2021 [52].

DeFi Protocol and Composability Attacks DeFi’s atomic composability can result in creative economic attacks (cf. Table 3). To our knowledge, “Value DeFi” is the target of the most severe composability attack on Ethereum, in which the adversary manipulated the price oracle in November 2020 to extract 740M USD in profit [54]. “PancakeBunny” suffered the to date most severe composability attack on the Binance Smart Chain in May 2020, resulting in a total loss of 45M USD [46].

DeFi Privacy While CeFi institutions are professionals at preserving their customer’s privacy, DeFi’s transparency discloses extensive information about the users’ assets and transactions. Therefore, multiple corporations offer services to governmental bodies, and law enforcement to trace and analyze blockchain-related financial transactions [21, 88]. Achieving privacy in DeFi hence appears as one of the most challenging future research directions. Related work goes as far as claiming an impossibility result on automated market makers [71].

5.4 CeFi vs. DeFi Market Manipulation

Market manipulation describes the act of intentional or willful conduct to deceive or defraud investors by controlling the price of financial instruments [45]. Market manipulation harms market fairness and honest traders’ rights and interests, regardless of whether the maleficent actor is the exchange or an internal/external trader.

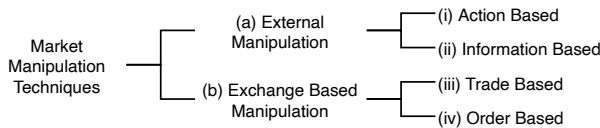


Figure 6: Classification of market manipulation techniques.

Market manipulations can be broadly classified into two categories based on whether they involve an exchange, namely (a) external manipulation and (b) exchange-based manipulation (cf.

Figure 6). Previous research has further classified market manipulations into four sub-categories [64, 171]: (i) Action-based, where the manipulator alters the actual or perceived value of the financial instrument without trading activities; (ii) Information-based manipulation, through the dissemination of false information or rumors. (iii) Trade-based manipulation, where a manipulator buys or sells financial instruments in a predetermined manner; and (iv) Order-based manipulation, where a manipulator cancels the placed orders before their execution.

It appears that action- and information-based manipulations are less reliant on the technical details of the underlying financial system. Therefore, external manipulation techniques for CeFi and DeFi are similar. However, exchange-based market manipulations, especially order-based HFT manipulations, rely heavily on the technical architecture. In Table 2, we present a taxonomy for DeFi related manipulation techniques. We omitted CeFi manipulation techniques that are not viable in DeFi⁴.

MEV and Market Manipulation as a Service Miner Extractable Value (MEV) can be captured by miners [96], as well as non-mining traders. When miners create a block, they have the unilateral power to momentarily decide what transactions to include, in what order. As a result, MEV extraction is frequently associated with trade-based market manipulation techniques like front-running [96], back-running [157], and sandwich attacks [191]. Worryingly, related work found that miners collaborate with centralized intermediaries to sell market manipulation as a service (MMAas) [35, 157]. Although MMAas lacks underlying principles or concepts of fairness and social benefits in general [122], at the time of writing this paper, there is no regulation prohibiting MEV extraction or market manipulations in DeFi.

Insight 6: DeFi Market Manipulations and the Wild Wild West

At the time of writing, world-wide regulations mostly do not account for the possible market manipulations feasible in DeFi, such as front-, back-running and sandwich attacks. As such, it appears that DeFi regulations remain at a state where CeFi was before the securities act of the year 1933.

6 Synergies between CeFi and DeFi

DeFi is still in its infancy. Due to the blockchain settlement layer, DeFi maintains unique properties to CeFi, such as non-custody, transparency, and decentralization. However, the blockchain also limits DeFi’s transaction throughput, transaction confirmation latency, and privacy. Ultimately, DeFi and CeFi share the same goal: to provide customers with high-quality financial products and services, and to power the entire economy. Summarizing, DeFi and CeFi each have their own set of advantages and disadvantages, and we cannot find a trivial way to combine the best of both systems. Therefore, we believe that these two distinct but intertwined financial systems will coexist and improve each other. In the following we present selected synergy opportunities.

⁴benchmark manipulation, wash sales, scalping, layering etc. [112, 113, 121, 136, 171]

Table 2: Taxonomy of market manipulation techniques. CeFi manipulation techniques that are not viable in DeFi are omitted.

Category	Technique	Differences compared with CeFi	References
Action-	Ponzi scheme	Payout rules are clearly written in smart contracts, which cannot be changed once deployed.	[77, 78, 89, 90, 143]
	Honeypot	A new type of market manipulation in DeFi that combine security issues with scams.	[175]
Info-	Fraudulent financial statements	On-chain data is transparent, but intermediaries may reveal fraudulent financial statements.	[109]
	Pump and dump/Short and distort	-	[110, 123, 133, 186]
Trade-	Wash trade/Matched orders/Painting the tape	CeFi exchanges can fabricate volume, while DeFi wash traders must pay transaction fees.	[66, 95, 158, 181]
	Insider trading	-	[67, 179]
	Cornering	-	-
	Capping	-	-
	Marking the close	DeFi does not have market opening or closing times.	-
	Front-/back-running, sandwich	Blockchain transaction orders are enforced by miners, which can be bribed.	[96, 157, 189, 191]
	Clogging/ Jamming	Clogging on the blockchain was used to win gambling applications.	[157]
	Churning	A centrally governed DeFi application may misuse users' assets to generate excessive fees.	-
Order-	Ramping/Advancing the bid/ Reducing the ask	In DeFi, transaction fees may deter an adversary from these practices.	-
	Spoofing/Pinging	These attacks are nearly free of cost on the DeFi network layer.	[172]
	Quote stuffing	Related works observed quote stuffing through back-run flooding.	[190]

6.1 Bridges

Financial institutions are bridging DeFi and CeFi to improve their efficiency. Oracles such as Chainlink transfer CeFi data to DeFi [173]; Synthetix allows users to trade CeFi financial instrument as derivatives on DeFi [174]; and the Grayscale Bitcoin Trust enables users to trade Bitcoin on CeFi over-the-counter market (OTCQX) [26].

6.2 DeFi: An Innovative Addition to CeFi

We observe that DeFi protocols not only copy fundamental CeFi services, but optimize them to the unique blockchain properties. For example, a new exchange mechanism called Automated Market Maker (AMM) [191] replaces in DeFi the prevalent order-book model of CeFi. An AMM is a smart contract that takes assets from liquidity providers. Traders hence trade against the AMM smart contract instead of interacting with liquidity providers directly. The AMM design requires fewer interactions from the market makers than a CeFi order book, which reduces transaction costs. We notice that CeFi is absorbing such innovations in turn. Centralized exchanges (e.g., Binance) start to provide market making services following an AMM model [56]. Certain CeFi markets, such as FX have employed a blend of the AMM model with human intervention, are well-positioned to enter the market-making business in DeFi, while incumbent DeFi AMM providers may adopt some of the CeFi techniques to reduce their customers' exposure to arbitrageurs [153]. We anticipate more innovative DeFi protocols, e.g., liquidity mining and lending pools with algorithmic interest rates, will be ported over to CeFi in the near future.

6.3 DeFi Collapse: A Lesson for CeFi?

On the 12th of March, 2020, the cryptocurrency market collapsed, with the ETH price declining over 30% within 24 hours [18]. On the 19th of May, 2021, the ETH price again dropped by more than 40% [11]. CeFi markets experienced a similar degree of distress (although with less extreme daily movements), with the Dow Jones Industrial Average declining by 9.99%, with the day earning the name of "Black Thursday".

Both CeFi and DeFi experienced severe stress throughout these crashes. Centralized exchange services were interrupted due to an unprecedented number of trading activities (e.g., Coinbase halted trading for over one hour [6]) and exchanges were temporarily

closed down after hitting pre-determined daily movement limits [94]. Similarly, on Ethereum, the gas price increased sharply, to the point that a regular ETH transfer costed over one hundred USD. The resulting network congestion delayed the confirmation of users' transactions and caused the failure of MakerDAO liquidation bots [32] in February 2020. Unlike CeFi, DeFi services are technically always available because of the distributive nature of blockchains. However, in the aforementioned extreme cases, the DeFi systems become prohibitively expensive for most users. Since then, more attention was given to the robustness of DeFi protocols [31].

Although CeFi and DeFi have different settlement mechanisms and user behaviors, DeFi's stress tests may be invaluable lessons for CeFi. While CeFi relies on circuit-breakers to ease excessive asset volatility [4] (markets halt trading upon volatility beyond custom thresholds), DeFi has to date apparently well coped without such interruptions and may help CeFi to better understand its limits.

Who's responsible? The presence of a centralized counterparty in CeFi, puts an implicit degree of responsibility on the central counterparty to maintain an orderly marketplace. Although not specifically codified, there is an implicit market expectation, built over the recent years, that the central bank will step at in times of severe crashes, either through verbal support, or through increasing the supply of money (lowering the central bank interest rates or printing more money through repurchases of government debt) to support asset prices. For example, in March 2020, the Federal Reserve drastically expanded money supply, slashed interest rates to near-zero, prompting a rapid recovery in equity prices. By contrast, in DeFi, there is no such central counterparty responsible for supporting asset prices in times of crises, and the closest equivalent to the CeFi mechanism are "show of confidence" measured by cryptocurrency influencers — founders of major cryptocurrencies, social media influencers, exchanges, and well-regarded adopters. Market crashes can be extremely destructive to the economic well-being of a society, and through history of CeFi market participants have sought to reduce the incidence of crashes. DeFi, so far, has gone through fewer crashes, and is likely to need to adopt some of the CeFi crash-prevention features as it gains mainstream adoption.

Insight 7: CeFi and DeFi

We expect CeFi and DeFi to co-exist, to complement, to strengthen and to learn from each others' experiences, mistakes and innovations. CeFi and DeFi are already today tightly intertwined (e.g., through centrally controllable stablecoins) and have jointly allowed the onboarding of a wider (e.g., technical) user demographic.

7 Conclusion

Under the above scrutiny, CeFi and DeFi may not appear as different as one might expect. The most prevalent distinguishing features are (i) who controls the assets, (ii) how transparent and accountable is the system, and (iii) what privacy protections exist for the end user? In this work, we provide a first taxonomy to objectively differentiate among CeFi and DeFi systems, its services, and ultimately find that DeFi already deeply incorporates CeFi assets (e.g., USD-C/USDT stablecoins) and practices (such as market manipulations). We ultimately hope that this work provides a bridge for both the CeFi and the DeFi audiences, to work together, learn from each others' mistakes towards constructing resilient, user friendly and efficient financial ecosystems.

Acknowledgments

The authors would like to thank Philipp Jovanovic for providing helpful comments on an earlier version as well as Xihan Xiong for collecting DeFi attacks in Table 3.

References

- [1] Analysis: Proposed fatf guidance for virtual assets and vasp - ciphertrace. <https://ciphertrace.com/analysis-proposed-fatf-guidance-for-virtual-assets-and-vasps/>.
- [2] Anti-money laundering regulation for all crypto exchanges on austrac's wish list | zdnet. <https://www.zdnet.com/article/anti-money-laundering-regulation-for-all-crypto-exchanges-on-austracs-wish-list/>.
- [3] China crypto mining business hit by beijing crackdown, bitcoin tumbles. <https://www.reuters.com/world/china/crypto-miners-halt-china-business-after-beijings-crackdown-bitcoin-dives-2021-05-24/>.
- [4] Circuit breaker definition. <https://www.investopedia.com/terms/c/circuitbreaker.asp>.
- [5] Coinbase. <https://www.coinbase.com>.
- [6] Coinbase, binance outage: exchanges go offline during crypto sell-off | fortune. <https://fortune.com/2021/05/19/coinbase-binance-outage-crypto-bitcoin-crash/>.
- [7] Coinbase wallet. <https://wallet.coinbase.com>.
- [8] Cover protocol. <https://www.coverprotocol.com/>.
- [9] Credit definition. <https://www.investopedia.com/terms/c/credit.asp>.
- [10] Creditworthiness definition. <https://www.investopedia.com/terms/c/creditworthiness.asp>.
- [11] The crypto collapse: Here's what's behind bitcoin's sudden drop. <https://www.cnbc.com/2021/05/19/the-crypto-collapse-heres-whats-behind-bitcoins-sudden-drop.html>.
- [12] Crypto lending rates - earn crypto interest by defi lending. <https://defirate.com/lend/>.
- [13] Curve.fi. <https://curve.fi/>.
- [14] Decentralized finance needs regulatory clarity and smarter compliance. <https://www.withersworldwide.com/en-gb/insight/decentralized-finance-needs-regulatory-clarity-and-smarter-compliance>.
- [15] Defi deep dive - what is the bzx protocol? <https://academy.ivanontech.com/blog/defi-deep-dive-what-is-the-bzx-protocol>.
- [16] Defi project akropolis drained of \$2m in dai. <https://www.coindesk.com/defi-project-akropolis-token-pool-drained>.
- [17] Defi status report post-black thursday - defi pulse. <https://www.starlink.com>.
- [18] Defi status report post-black thursday - defi pulse. <https://defipulse.com/blog/defi-status-report-black-thursday/#:~:text=On%20Thursday%20March%2012%2C%202020,%2C%20bolstering%20collateral%20ratio%2C%20etc>.
- [19] Documents - financial action task force (fatf). <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>.
- [20] Eip-20: Erc-20 token standard. <https://eips.ethereum.org/EIPS/eip-20>.
- [21] Elliptic. <https://www.elliptic.co>.
- [22] Ethermine. <https://ethermine.org>.
- [23] Fatf-gafi.org - financial action task force (fatf). <https://www.fatf-gafi.org/>.
- [24] Fatf's new guidance takes aim at defi - coindesk. <https://www.coindesk.com/fatfs-new-guidance>.
- [25] The future of client onboarding - fintech futures. <https://www.fintechfutures.com/2018/09/the-future-of-client-onboarding/>.
- [26] Grayscale bitcoin trust. <https://grayscale.com/products/grayscale-bitcoin-trust/>.
- [27] Home - alpha finance lab. <https://alphafinance.io>.
- [28] Home | prevent flash loan attacks. <https://preventflashloanattacks.com/>.
- [29] How did lendf.me lose \$25 million to a reentrancy attack? [an analysis]. <https://hackernoon.com/how-did-lendfme-lose-dollar25-million-to-a-reentrancy-attack-an-analysis-091iy32s7>.
- [30] Infura. <https://infura.io>.
- [31] Liquidations 2.0: Technical summary - governance / proposal ideas - the maker forum. <https://forum.makerdao.com/t/liquidations-2-0-technical-summary/4632>.
- [32] The market collapse of march 12-13, 2020: How it impacted makerdao. <https://blog.makerdao.com/the-market-collapse-of-march-12-2020-how-it-impacted-makerdao/>.
- [33] Market dynamics of the 1st bzx hack: Flash loans and the insolvent loan. <https://quantstamp.com/blog/market-dynamics-of-the-1st-bzx-hack-part-1>.
- [34] Metamask. <https://metamask.io/>.
- [35] Mev monster. <https://mev.monster>.
- [36] ML 7.1 the money laundering reporting officer - fca handbook. <https://www.handbook.fca.org.uk/handbook/ML/7/1.html?date=2005-04-02>.
- [37] Monetary policy: Stabilizing prices and output - back to basics: Finance & development. <https://www.imf.org/external/pubs/ft/fandd/basics/monopol.htm>.
- [38] Nasdaq. <https://www.nasdaq.com>.
- [39] New fatf draft guidance to regulate p2p transfers, defi, dexts, nft and stablecoins - sygna. <https://www.sygna.io/blog/fatf-draft-guidance-on-rba-to-virtual-assets-and-vasps-public-consultation-march-2021/>.
- [40] Origin dollar incident: Root cause analysis. <https://peckshield.medium.com/origin-dollar-incident-root-cause-analysis-f27e11988c90>.
- [41] Outages continue to plague online brokerages - wsj. <https://www.wsj.com/articles/outages-continue-to-plague-online-brokerages-11611768827>.
- [42] Paid network exploit mints attacker 60m tokens: Report. <https://www.coindesk.com/paid-network-exploit-mints-attacker-60m-tokens-report>.
- [43] Risk-free rate of return definition. <https://www.investopedia.com/terms/r/risk-free-rate.asp>.
- [44] Robinhood restricts trading in gamestop, other names involved in frenzy. <https://www.cnbc.com/2021/01/28/robinhood-interactive-brokers-restrict-trading-in-gamestop-s.html>.
- [45] Sec market manipulation and case studies. <https://www.sec.gov/files/Market%20Manipulations%20and%20Case%20Studies.pdf>.
- [46] Slowmist: Pancakebunny hack analysis. <https://slowmist.medium.com/slowmist-pancakebunny-hack-analysis-4a708e284693>.
- [47] Sparkpool. <https://www.sparkpool.com>.
- [48] Sr 955.0 - federal act of 10 october 1997 on combating money laundering and terrorist financing in the financial sector (anti-money laundering act, amla). https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en.
- [49] Tornado anonymity mining. <https://app.tornado.cash/mining/>.
- [50] Tornado.cash. <https://tornado.cash/>.
- [51] United states government bonds - yields curve. <http://www.worldgovernmentbonds.com/country/united-states/>.
- [52] Uranium finance - rekt. <https://www.rekt.news/uranium-rekt/>.
- [53] U.s. bank savings account rates | bankrate. <https://www.bankrate.com/banking/savings/us-bank-savings-rates/>.
- [54] Value defi incident: Root cause analysis. <https://blog.peckshield.com/2020/11/15/valuedefi/>.
- [55] What exactly is a virtual asset service provider (vasp)? - ciphertrace. <https://ciphertrace.com/what-exactly-is-a-virtual-asset-service-provider-vasp/#:~:text=When%20a%20digital%20asset%20entity,role%20as%20a%20money%20tr>.
- [56] What is liquid swap? | binance support. <https://www.binance.com/en/support/faq/85d614205d334128b76c0275aba61ea6>.
- [57] What is the hong kong-us dollar peg and how does it work? - yp | south china morning post. <https://www.scmp.com/yp/discover/advice/article/3093224/what-hong-kong-us-dollar-peg-and-how-does-it-work>.

- [58] What is the risk-free rate of return? <https://www.thebalance.com/what-is-risk-free-rate-of-return-5097109>.
- [59] Why trump administration threat to hurt hong kong's dollar peg won't work. <https://www.cnn.com/2020/07/13/why-trump-administration-threat-to-hurt-hong-kongs-dollar-peg-wont-work.html#:~:text=The%20Hong%20Kong%20dollar%20has,selling%20or%20buying%20the%20currency>.
- [60] Foreign exchange manipulation: FINMA issues six industry bans, 2019.
- [61] Aave. Aave Protocol. <https://github.com/aave/aave-protocol>, 2020.
- [62] Hamda Al-Breiki, Muhammad Habib Ur Rehman, Khaled Salah, and Davor Svetinovic. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access*, 8:85675–85685, 2020.
- [63] Irene Aldridge. *High-frequency trading: a practical guide to algorithmic strategies and trading systems*, volume 604. John Wiley & Sons, 2013.
- [64] Franklin Allen and Douglas Gale. Stock-price manipulation. *The Review of Financial Studies*, 5(3):503–529, 1992.
- [65] Sarah Allen, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostianen, Sarah Meiklejohn, Andrew Miller, et al. Design choices for central bank digital currency: Policy and technical considerations. Technical report, National Bureau of Economic Research, 2020.
- [66] Arash Aloosh and Jiasun Li. Direct evidence of bitcoin wash trading. *Available at SSRN 3362153*, 2019.
- [67] John P Anderson. Insider trading and cryptoassets: The waters just got muddier. *Iowa L. Rev. Bull.*, 104:120, 2019.
- [68] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srđjan Čapkun. Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer, 2013.
- [69] James J Angel and Douglas McCabe. Fairness in financial markets: The case of high frequency trading. *Journal of Business Ethics*, 112(4):585–595, 2013.
- [70] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. *arXiv preprint arXiv:2003.10001*, 2020.
- [71] Guillermo Angeris, Alex Evans, and Tarun Chitra. A note on privacy in constant function market makers. *arXiv preprint arXiv:2103.01193*, 2021.
- [72] Jun Aoyagi. Strategic Speed Choice by High-Frequency Traders under Speed Bumps. *ISER DP*, (1050), 2019.
- [73] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 375–392. IEEE, 2017.
- [74] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust*, pages 164–186. Springer, 2017.
- [75] European Central Bank. Monetary Policy. <https://www.ecb.europa.eu/mopo/html/index.en.html>, 2021.
- [76] Matthew Baron, Jonathan Brogaard, Björn Hagströmer, and Andrei Kirilenko. Risk and return in high-frequency trading. *Journal of Financial and Quantitative Analysis*, 54(3):993–1024, 2019.
- [77] Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. Dissecting ponzi schemes on ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 102:259–277, 2020.
- [78] Massimo Bartoletti, Barbara Pes, and Sergio Serusi. Data mining for detecting bitcoin ponzi schemes. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 75–84. IEEE, 2018.
- [79] Abdeljalil Beniche. A study of blockchain oracles. *arXiv preprint arXiv:2004.07140*, 2020.
- [80] Iddo Bentov, Yan Ji, Fan Zhang, Lorenz Breidenbach, Philip Daian, and Ari Juels. Tesseract: Real-time cryptocurrency exchange using trusted hardware. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1521–1538, 2019.
- [81] Iddo Bentov, Yan Ji, Fan Zhang, Yunqi Li, Xueyuan Zhao, Lorenz Breidenbach, Philip Daian, and Ari Juels. Tesseract: Real-Time Cryptocurrency Exchange using Trusted Hardware. *Conference on Computer and Communications Security*, 2019.
- [82] Daniele Bianchi and Alexander Dickerson. Trading volume in cryptocurrency markets. *Available at SSRN 3239670*, 2019.
- [83] Lorenz Breidenbach, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, Farinaz Koushanfar, Andrew Miller, Brendan Magauran, Daniel Moroz, et al. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. 2021.
- [84] Jonathan Brogaard et al. High frequency trading and its impact on market quality. *Northwestern University Kellogg School of Management Working Paper*, 66, 2010.
- [85] Eric Budish, Peter Cramton, and John Shim. The high-frequency trading arms race: Frequent batch auctions as a market design response. *The Quarterly Journal of Economics*, 130(4):1547–1621, 2015.
- [86] Tong Cao. Paradox of Inflation: The Study on Correlation between Money Supply and Inflation in New Era. <https://core.ac.uk/download/pdf/79576314.pdf>, 2015.
- [87] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167, 2016.
- [88] Chainalysis. Decoding increasingly sophisticated hacks, darknet markets, and scams. Technical report, 2019.
- [89] Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In *Proceedings of the 2018 World Wide Web Conference*, pages 1409–1418, 2018.
- [90] Weili Chen, Zibin Zheng, Edith C-H Ngai, Peilin Zheng, and Yuren Zhou. Exploiting blockchain data to detect smart ponzi schemes on ethereum. *IEEE Access*, 7:37575–37586, 2019.
- [91] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 185–200. IEEE, 2019.
- [92] Michael Christalla, Bernhard Speyer, Sabine Kaiser, and Thomas Mayer. High-frequency trading. *Deutsche Bank Research*, 7:3–4, 2011.
- [93] Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers. Fairness in an unfair world: Fair multiparty computation from public bulletin boards. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 719–728, 2017.
- [94] CNBC, Bloom Michael, Cox Jeff, and Franck Thomas. ‘Circuit breaker’ triggered again to keep stocks from falling through floor. <https://www.cnn.com/2020/03/12/stock-futures-hit-a-limit-down-trading-halt-for-a-second-time-this-week-heres-what-that-means.html>, 2020.
- [95] Lin William Cong, Xi Li, Ke Tang, and Yang Yang. Crypto wash trading. *Available at SSRN 3530220*, 2020.
- [96] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *arXiv preprint arXiv:1904.05234*, 2019.
- [97] Barry J Eichengreen, Barry Eichengreen, and Marc Flandreau. *The gold standard in theory and history*. Psychology press, 1997.
- [98] Parinya Ekparinya, Vincent Gramoli, and Guillaume Jourjon. Impact of man-in-the-middle attacks on ethereum. In *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, pages 11–20. IEEE, 2018.
- [99] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*, pages 436–454. Springer, 2014.
- [100] Frank J Fabozzi and Pamela Peterson Drake. What is finance. *FRANK J. FABOZZI PAMELA PETERSON DRAKE*, 3, 2009.
- [101] St Louis Fed. M1 Money Stock. <https://fred.stlouisfed.org/series/M1>, 2021.
- [102] Compound Finance. Compound finance. <https://compound.finance/>, 2019.
- [103] The Maker Foundation. Makerdao. <https://makerdao.com/en/>, 2019.
- [104] Arthur Gervais, Srđjan Čapkun, Ghassan O Karame, and Damian Gruber. On the privacy provisions of bloom filters in lightweight bitcoin clients. In *Computer Security Applications Conference*, pages 326–335, 2014.
- [105] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srđjan Čapkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16. ACM, 2016.
- [106] Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and Srđjan Čapkun. Tampering with the delivery of blocks and transactions in bitcoin. In *Conference on Computer and Communications Security*, pages 692–705. ACM, 2015.
- [107] Globalcustodian.com. Global Custodians. <https://www.globalcustodian.com/directory-type/global-custodians/>, 2021.
- [108] Johannes Göbel, Holger Paul Keeler, Anthony E Krzesinski, and Peter G Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104:23–41, 2016.
- [109] John M Griffin and Amin Shams. Is bitcoin really untethered? *The Journal of Finance*, 75(4):1913–1964, 2020.
- [110] JT Hamrick, Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek. The economics of cryptocurrency pump and dump schemes. 2018.
- [111] Mark Handley. Delay is not an option: Low latency routing in space. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, pages 85–91, 2018.
- [112] Jon D Hanson and Douglas A Kysar. Taking behavioralism seriously: Some evidence of market manipulation. *Harvard law review*, pages 1420–1572, 1999.
- [113] Jon D Hanson and Douglas A Kysar. Taking behavioralism seriously: The problem of market manipulation. *NYUL Rev*, 74:630, 1999.
- [114] Martin Harrigan and Christoph Fretter. The unreasonable effectiveness of address clustering. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pages 368–373. IEEE,

- 2016.
- [115] Martin Harrigan, Lei Shi, and Jacob ILLUM. Airdrops and privacy: a case study in cross-blockchain analysis. In *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pages 63–70. IEEE, 2018.
 - [116] Larry Harris. What to do about high-frequency trading, 2013.
 - [117] Eyal Hertzog, Guy Benartzi, and Galia Benartzi. Bancor protocol. 2017.
 - [118] Abraham Hinteregger and Bernhard Haslhofer. An Empirical Analysis of Monero Cross-Chain Traceability. *CoRR*, abs/1812.02808, 2018.
 - [119] Investopedia. Basket of Goods. https://www.investopedia.com/terms/b/basket_of_goods.asp, 2021.
 - [120] Investopedia. Inflation. <https://www.investopedia.com/terms/i/inflation.asp>, 2021.
 - [121] Robert A Jarrow. Market manipulation, bubbles, corners, and short squeezes. *Journal of financial and Quantitative Analysis*, 27(3):311–336, 1992.
 - [122] Ari Juels, Ittay Eyal, and Mahimna Kelkar. Op-ed: Miners, front-running-as-a-service is theft. <https://mev.monster>.
 - [123] Josh Kamps and Bennett Kleinberg. To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, 7(1):1–18, 2018.
 - [124] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 906–917. ACM, 2012.
 - [125] Ghassan O Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Capkun. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, 18(1):2, 2015.
 - [126] Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas. Fair and robust multi-party computation using a global transaction ledger. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 705–734. Springer, 2016.
 - [127] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*, pages 839–858. IEEE, 2016.
 - [128] Peter Koudijs and Hans-Joachim Voth. Leverage and beliefs: personal experience and risk-taking in margin lending. *American Economic Review*, 106(11):3367–3400, 2016.
 - [129] Aurora Labs. IDEX: A real-time and high-throughput ethereum smart contract exchange. Technical report, January 2019.
 - [130] Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaide, and Thomas Engel. Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, pages 87–94, 2014.
 - [131] CFA Larry Harris, PhD. STRUCTURE OF THE INVESTMENT INDUSTRY. <https://www.cfainstitute.org/-/media/documents/support/programs/investment-foundations/13-structure-of-the-investment-industry.ashx>, 2021.
 - [132] Duc V Le and Arthur Gervais. Amr: Autonomous coin mixer with privacy preserving reward distribution. *arXiv preprint arXiv:2010.01056*, 2020.
 - [133] Tao Li, Donghua Shin, and Baolian Wang. Cryptocurrency pump-and-dump schemes. *Available at SSRN 3267041*, 2020.
 - [134] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107:841–853, 2020.
 - [135] Iuon-Chang Lin and Tzu-Chun Liao. A survey of blockchain security issues and challenges. *IJ Network Security*, 19(5):653–659, 2017.
 - [136] Tom CW Lin. The new market manipulation. *Emory LJ*, 66:1253, 2016.
 - [137] Joshua Lind, Ittay Eyal, Peter Pietzuch, and Emin Gün Sirer. Teechain: Payment channels using trusted execution environments. *arXiv preprint arXiv:1612.07766*, 2016.
 - [138] Joshua Lind, Oded Naor, Ittay Eyal, Florian Kelbert, Peter R Pietzuch, and Emin Gün Sirer. Teechain: Reducing Storage Costs on the Blockchain With Offline Payment Channels. In *Proceedings of the 11th [ACM] International Systems and Storage Conference, [SYSTOR] 2018, HAIFA, Israel, June 04-07, 2018*, 2018.
 - [139] Bowen Liu, Pawel Szalachowski, and Jianying Zhou. A first look into defi oracles. *arXiv preprint arXiv:2005.04377*, 2020.
 - [140] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.
 - [141] Albert J Menkveld. The economics of high-frequency trading: Taking stock. *Annual Review of Financial Economics*, 8:1–24, 2016.
 - [142] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Symposium on Security and Privacy*, pages 397–411, 2013.
 - [143] Tian Min, Hanyi Wang, Yaoze Guo, and Wei Cai. Blockchain games: A survey. In *2019 IEEE Conference on Games (CoG)*, pages 1–8. IEEE, 2019.
 - [144] Amani Moin, Kevin Sekniqi, and Emin Gün Sirer. Sok: A classification framework for stablecoin designs. In *International Conference on Financial Cryptography and Data Security*, pages 174–197. Springer, 2020.
 - [145] John V Monaco. Identifying bitcoin users by transaction behavior. In *Biometric and Surveillance Technology for Human and Activity Identification XII*, volume 9457, page 945704. International Society for Optics and Photonics, 2015.
 - [146] Wouter H Muller, Christian H Kalin, and John G Goldsworth. *Anti-Money Laundering: international law and practice*. John Wiley & Sons, 2007.
 - [147] Nexus Mutual. Nexus Mutual. <https://nexusmutual.io/>, 2020.
 - [148] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. *Bitcoin*. URL: <https://bitcoin.org/bitcoin.pdf>, 4, 2008.
 - [149] Nasdaq. Initial Listing Guide. <https://listingcenter.nasdaq.com/assets/initialguidede.pdf>, 2021.
 - [150] Till Neudecker and Hannes Hartenstein. Could network information facilitate address clustering in bitcoin? In *International conference on financial cryptography and data security*, pages 155–169. Springer, 2017.
 - [151] Mardiana Mohamad Noor and Wan Haslina Hassan. Wireless networks: developments, threats and countermeasures. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 3(1):125–140, 2013.
 - [152] Bank of England. Inflation and the 2 percent target. <https://www.bankofengland.co.uk/monetary-policy/inflation>, 2021.
 - [153] Bank of International Settlements. FX execution algorithms and market functioning. <https://www.bis.org/publ/mkctc13.pdf>, 2020.
 - [154] US Bureau of Labor Statistics. Consumer prices increase 2.6 percent for the 12 months ending March 2021. <https://www.bls.gov/opub/ted/2021/consumer-prices-increase-2-6-percent-for-the-12-months-ending-march-2021.htm>, 2021.
 - [155] Financial Conduct Authority of the UK. Primary Markets. <https://www.fca.org.uk/markets/primary-markets>, 2021.
 - [156] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: scalable off-chain instant payments, 2016.
 - [157] Kaihua Qin, Liyi Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? *arXiv preprint arXiv:2101.05511*, 2021.
 - [158] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the defi ecosystem with flash loans for fun and profit. *Financial Cryptography and Data Security: 25th International Conference (FC 2021)*, 2021.
 - [159] Venkatesh U Rajput. Research on know your customer (kyc). *International Journal of Scientific and Research Publications*, 3(7):541–546, 2013.
 - [160] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.
 - [161] Hubert Ritzdorf, Karl Wüst, Arthur Gervais, Guillaume Felley, and Srdjan Capkun. TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing. In *NDSS*, 2018.
 - [162] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and Aziz Mohaisen. Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv:1904.03487*, 2019.
 - [163] Muhammad Saad, My T Thai, and Aziz Mohaisen. Poster: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 809–811, 2018.
 - [164] Ayelet Sapirshstein, Yonatan Sompolsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.
 - [165] Corina Sas and Irni Eliana Khairuddin. Design for trust: An exploration of the challenges and opportunities of bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6499–6510, 2017.
 - [166] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 459–474. IEEE, 2014.
 - [167] Sarwar Sayeed and Hector Marco-Gisbert. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, 9(9):1788, 2019.
 - [168] Fabian Schär. Decentralized finance: On blockchain-and smart contract-based financial markets. *Available at SSRN 3571335*, 2020.
 - [169] Linda Schilling and Harald Uhlig. Some simple bitcoin economics. *Journal of Monetary Economics*, 106:16–26, 2019.
 - [170] Paul Allan Schott. *Reference guide to anti-money laundering and combating the financing of terrorism*. World Bank Publications, 2006.
 - [171] Michael Siering, Benjamin Clapham, Oliver Engel, and Peter Gombor. A taxonomy of financial market manipulations: establishing trust and market integrity in the financialized economy through automated fraud detection. *Journal of Information Technology*, 32(3):251–269, 2017.
 - [172] Antoon Spithoven. Theory and reality of cryptocurrency governance. *Journal of Economic Issues*, 53(2):385–393, 2019.
 - [173] Sergey Nazarov Steve Ellis, Ari Juels. Chainlink: A decentralized oracle network, 2017.
 - [174] Synthetix. Synthetix: Decentralized synthetic assets. <https://www.synthetix.io/>, 2020.
 - [175] Christof Ferreira Torres, Mathis Steichen, et al. The art of the scam: Demystifying honeypots in ethereum smart contracts. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 1591–1607, 2019.

- [176] Tradingview. Random length lumber futures. <https://www.tradingview.com/chart/?symbol=CME%3ALBS1!>, 2021.
- [177] European Union. Payments, Transfers, and Cheques. https://europa.eu/youreurope/citizens/consumers/financial-products-and-services/payments-transfers-cheques/index_en.htm, 2021.
- [178] Uniswap.io, 2018. <https://docs.uniswap.io/>.
- [179] Andrew Verstein. Crypto assets and insider trading law’s domain. *Iowa L. Rev.*, 105:1, 2019.
- [180] Friedhelm Victor. Address clustering heuristics for ethereum. In *International Conference on Financial Cryptography and Data Security*, pages 617–633. Springer, 2020.
- [181] Friedhelm Victor and Andrea Marie Weintraud. Detecting and quantifying wash trading on decentralized cryptocurrency exchanges. *arXiv preprint arXiv:2102.07001*, 2021.
- [182] Christopher Viney and Peter Phillips. *Financial institutions, instruments & markets*. McGraw-Hill Australia, 2012.
- [183] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. Towards understanding flash loan and its applications in defi ecosystem. *arXiv preprint arXiv:2010.12252*, 2020.
- [184] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain. URL: <https://github.com/0xProject/whitepaper>, pages 04–18, 2017.
- [185] Karl Wüst and Arthur Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.
- [186] Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency pump-and-dump scheme. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1609–1625, 2019.
- [187] Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 270–282. ACM, 2016.
- [188] Fan Zhang, Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. Deco: Liberating web data using decentralized oracles for tls. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1919–1938, 2020.
- [189] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of profit-generating transactions in defi protocols. *2021 IEEE Symposium on Security and Privacy (SP)*, 2021.
- [190] Liyi Zhou, Kaihua Qin, and Arthur Gervais. A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges. 2021.
- [191] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. High-frequency trading on decentralized on-chain exchanges. *2021 IEEE Symposium on Security and Privacy (SP)*, 2020.

Table 3: Smart contract code and DeFi protocol/composability attacks on Ethereum as well as the Binance Smart Chain.

Victim	Amount (USD)	Platform	Source
The DAO	60,000,000	ETH	https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
Parity	30,000,000	ETH	https://medium.com/solidified/parity-hack-how-it-happened-and-its-aftermath-9bffb2105c0
Bancor	23,500,000	ETH	https://medium.com/@theoceantrade/hack-attack-volume-3-bancor-55abfa9aef2
Spankchain	38,000	ETH	https://medium.com/swlh/how-spankchain-got-hacked-af65b933393c
bZx	355,880	ETH	https://blog.peckshield.com/2020/02/17/bZx/
bZx	665,840	ETH	https://blog.peckshield.com/2020/02/18/bZx/
Lendf.Me	25,236,849	ETH	https://blog.peckshield.com/2020/04/19/erc777/
Bancor	135,229	ETH	https://blog.bancor.network/bancors-response-to-today-s-smart-contract-vulnerability-dc888c589fe4
Balancer	523,617	ETH	https://blog.peckshield.com/2020/06/28/balancer/
Balancer	2,408	ETH	https://cointelegraph.com/news/hacker-steals-balancers-comp-allowance-in-second-attack-within-24-hours
VETH	900,000	ETH	https://hacked.slowmist.io/en/?c=ETH%20DApp
Opyn	371,000	ETH	https://blog.peckshield.com/2020/08/05/opyn/
YFValue	170,000,000	ETH	https://valuedefi.medium.com/yfv-update-staking-pool-exploit-713cb353ff7d
SoftFinance	250,000	ETH	https://cointelegraph.com/news/jackpot-user-turns-200-into-250k-thanks-to-a-buggy-defi-protocol
Uniswap	220,000	ETH	https://medium.com/consensus-diligence/uniswap-audit-b90335ac007
Soda.Finance	160,000	ETH	https://anchainai.medium.com/soda-finance-hack-could-formal-verification-have-prevented-it-code-included-71b6e9f94ea5
Eminence	15,000,000	ETH	https://www.rekt.news/eminence-rekt-in-prod/
DeFi Saver	30,000	ETH	https://slowmist.medium.com/slowmist-how-was-the-310-000-dai-of-defi-saver-users-stolen-91de37a4ade2
Harvest Finance	33,800,000	ETH	https://www.rekt.news/harvest-finance-rekt/
Axon Network	500,000	ETH	https://cointelegraph.com/news/certik-dissects-the-axon-network-incident-and-subsequent-price-crash
Cheese Bank	3,300,000	ETH	https://blog.peckshield.com/2020/11/16/cheesebank/
Akropolis	2,030,000	ETH	https://blog.peckshield.com/2020/11/13/akropolis/
ValueDeFi	740,000,000	ETH	https://blog.peckshield.com/2020/11/15/valuedefi/
OUSD	7,700,000	ETH	https://blog.peckshield.com/2020/11/17/ousd/
88mph	100,000	ETH	https://peckshield.medium.com/88mph-incident-root-cause-analysis-ce477e00a74d
Pickle.Finance	20,000,000	ETH	https://www.rekt.news/pickle-finance-rekt/
SushiSwap	15,000	ETH	https://slowmist.medium.com/slowmist-a-brief-analysis-of-the-story-of-the-sushi-swap-attack-c7bc6709adea
Warp.Finance	7,800,000	ETH	https://blog.peckshield.com/2020/12/18/warpfinance/
Nexus Mutual	8,000,000	ETH	https://www.certik.io/blog/technology/nexus-mutual-attack-8-million-lost
Cover Protocol	3,000,000	ETH	https://blog.peckshield.com/2020/12/28/cover/
SushiSwap	103,842	ETH	https://www.rekt.news/badgers-digg-sushi/
BT.Finance	1,500,000	ETH	https://www.rekt.news/the-big-combo/
Yearn.Finance	11,000,000	ETH	https://www.rekt.news/yearn-rekt/
Cream.Finance	37,500,000	ETH	https://www.rekt.news/alpha-finance-rekt/
Meerkat Finance	31,000,000	BSC	https://www.rekt.news/meerkat-finance-bsc-rekt/
Paid Network	27,418,034	ETH	https://www.rekt.news/paid-rekt/
Furucombo	15,000,000	ETH	https://www.rekt.news/furucombo-rekt/
Iron.Finance	170,000	BSC	https://ironfinance.medium.com/iron-finance-vfarms-incident-post-mortem-16-march-2021-114e58d1eaac
Uranium.Finance	13,000,000	BSC,ETH	https://www.certik.org/blog/uranium-finance-exploit-technical-analysis
PancakeSwap	1,800,000	BSC	https://cryptopwnage.medium.com/1-800-000-was-stolen-from-binance-smart-chain-pancakeswap-lottery-pool-ca2afb415f9
Uranium.Finance	57,200,000	BSC,ETH	https://www.rekt.news/uranium-rekt/
Spartan	30,500,000	BSC	https://blog.peckshield.com/2021/05/02/Spartan/
ValueDeFi	10,000,000	BSC	https://www.rekt.news/value-rekt2/
EasyFi	59,000,000	Layer 2	https://www.rekt.news/easyfi-rekt/
ValueDeFi	11,000,000	BSC	https://blog.peckshield.com/2021/05/08/ValueDeFi/
Rari Capital	14,000,000	ETH	https://nipump.medium.com/5-8-21-rari-capital-exploit-timeline-analysis-8beda31cbc1a
xToken	24,000,000	ETH	https://medium.com/xtoken/initial-report-on-xbnta-xsnxa-exploit-d6e784387f8e
FinNexus	7,000,000	ETH,BSC	https://news.yahoo.com/latest-defi-hack-drains-7-050841516.html
PancakeBunny	45,000,000	BSC,ETH	https://slowmist.medium.com/slowmist-pancakebunny-hack-analysis-4a708e284693
Bogged Finance	3,600,000	BSC	https://blog.peckshield.com/2021/05/22/boggedfinance/
AutoShark Finance	822,800	BSC	https://authorshark.medium.com/
DeFi100	32,000,000	ETH	https://www.coindesk.com/people-behind-crypto-protocol-defi100-may-have-absconded-with-32m-in-investor-funds
WLEO	42,000	ETH	https://leofinance.io/@leofinance/wrapped-leo-white-paper-investigative-report-lp-refunds-and-wleo-relaunch
UniCats	200,000	ETH	https://hacked.slowmist.io/en/?c=ETH%20DApp
Web3 DeFi	100,000	ETH	https://medium.com/mycrypto/phishing-campaigns-take-aim-at-web3-defi-applications-19e224d9f207
bZx	8,000,000	ETH	https://bzx.network/blog/incident
MakerDAO	8,320,000	ETH	https://www.coindesk.com/mempool-manipulation-enabled-theft-of-8m-in-makerdao-collateral-on-black-thursday-report
Fomo 3D	18,000,000	ETH	https://blog.peckshield.com/2018/07/24/fomo3d/

Table 4: Definitions of DeFi market manipulation techniques.

Category	Technique	Definition
Action-	Ponzi scheme	An adversary raises funds from investors while paying to previous investors, creating the illusion of high returns.
	Honey pot	An adversary feigns a financial instrument, luring market participants into making erroneous trades.
Info-	Fraudulent financial statements	Intentional misrepresentation of a company's financial health via disclosure violations and improper accounting.
	Pump and dump/Short and distort	Adversary buying positions to increase the price, disseminating positive information, and then selling.
Trade-	Wash trade/Matched orders/Painting the tape	Creating fictitious transactions to imply market activity.
	Insider trading	Trading based on non-public information.
	Cornering	Obtaining a large quantity of a specific financial instrument to manipulate the market price.
	Capping	Preventing the rise/decrease in the financial instrument's price.
	Marking the close	Pumps or dumps the opening or closing price of an instrument.
	Front-/back-running, sandwich	Using pending information about incoming transaction to perform a financial action.
	Clogging/Jamming	Clogging the network to prevent other market participants from issuing transactions.
	Churning	Purchasing and selling of financial instruments on behalf of a client for profit.
Order-	Ramping/Advancing the bid/ Reducing the ask	In/decreasing the bid for an asset to artificially in/decrease its price, or to simulate an active asset interest.
	Spoofing/Pinging	Places trading orders that are not intended to be executed, to observe or mislead other participants'.
	Quote stuffing	Placing and canceling a many orders to overload a financial system, similar to a DoS attack.