DeFi Protocol Risks: the Paradox of DeFi[1]

By Nic Carter[2] and Linda Jeng[3]

Abstract

Decentralized Finance (or "DeFi") is growing in volume and in importance. DeFi promises cheaper and more open access to financial services by reducing the costs and risks of using centralized intermediaries. DeFi also holds the promise of interoperability across blockchains that could help tear down financial sector silos, greatly promoting innovation and building vibrant financial ecosystems. However, DeFi is not without its challenges, which are understudied. This article does not seek to provide a comprehensive list of DeFi but to help readers conceptually understand the drivers behind the risks inherent in DeFi. Many of the risks described above stem from the decentralized nature of blockchains. The goal of automating the delivery of financial services and reducing human dependencies also has the congruent effect of reducing oversight and control. Disintermediating traditional intermediaries reduces high fees and entry friction, but also creates new opportunities for new types of intermediaries. This article discusses some of the new types of risks introduced by DeFi that are inherent to blockchain systems along with traditional types of financial risks in DeFi that manifest in new ways: (i) interconnections with the traditional financial system, (ii) operational risks stemming from underlying blockchains, (iii) smart contract-based vulnerabilities, (iv) other governance and regulatory risks, and (v) scalability challenges. In an effort to remove humans and automate as much as possible through smart contracts, DeFi has introduced or amplified these risks. The growth of DeFi will depend on its ability to navigate and build compatibility with traditional finance and on how laws and regulations respond. Perhaps the biggest challenge of all is that the DeFi ecosystem continues to grow while its underlying base layer (public infrastructure such as Bitcoin or Ethereum) faces growing pains. As DeFi grows in importance and becomes more mainstream, policymakers and industry representatives need to better understand the economic and policy consequences of these new types of risks in order to build regulatory approaches and risk management practices that can support and facilitate a healthy and robust DeFi ecosystem and, ultimately, the financial stability of the greater financial system and real economy.

---

[1] This article will be included as part of a forthcoming book edited by Bill Coen and Diane Maurice "Regtech, Suptech and Beyond: Innovation and Technology in Financial Services" RiskBooks – forthcoming 3Q 2021. The authors wish to thank Jon Frost and Greg Xethalis for reviewing this chapter and for their invaluable feedback.

[2] Nic Carter is a General Partner at Castle Island Ventures (CIV), a seed-stage venture firm investing in startups building on public blockchains, and the co-founder of Coin Metrics, a blockchain analytics firm. *Disclaimer: CIV holds active liquid and illiquid positions in several decentralized finance tokens and startups. Disclaimer: All mentions of protocols, tokens, and digital assets in this chapter are merely exemplary and do not constitute endorsements*

[3] Linda Jeng is Visiting Scholar on Financial Technology at Georgetown University Law Center's Institute of International Economic Law. She is also the Global Head of Policy at Transparent Financial Systems. She has held various regulatory roles, including at the Federal Reserve Board, the Financial Stability Board, and the US Treasury Department.

1. Introduction

On February 16, 2021, the price of Bitcoin crossed $50,000 for the first time, doubling its value in less than two months.[4] Earlier in the year, a string of announcements by a number of Wall Street banks and traditional financial firms, including Bank of New York Mellon, Mastercard, and Blackrock, proclaimed that they would begin working with bitcoin. The companies Square and Tesla made splashes by investing a combined total of nearly $2 billion USD in bitcoin.[5] Meanwhile, Square's and PayPal's retail customers now buy an amount equivalent to a majority of the new supply of bitcoin entering the market each day.[6] Visa also unveiled a bitcoin and crypto plan to be launched later in 2021.[7] Crypto is becoming mainstream and is here to stay.

Decentralized finance (or "DeFi") is typically understood by crypto users and enthusiasts as platforms and protocols that seek to replicate existing financial services by using crypto/blockchain technology with limited centralization. CoinDesk defines DeFi as: "an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries." Fabian Schär defines it more specifically as "an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, such as the Ethereum blockchain."[8]

Central banks and financial regulators presently do not view the crypto market as being large enough to pose a significant threat to global financial stability.[9] However, this assessment does not discount the need for regulators, industry and academics to understand (1) what are the new emerging risks of DeFi and (2) how DeFi may be impacting the transmission of traditional financial risks. Crypto markets are not insignificant and can no longer be discounted as small. For example, at the time of writing, DeFi projects on Ethereum hold collateral having the value

---

[4] Vigna, Paul & Ostroff, Caitlin. "Bitcoin Trades Above $50,000 for First Time" Wall Street Journal (Feb. 16, 2021). https://www.wsj.com/articles/bitcoin-trades-above-50-000-for-first-time-11613479752

[5] Son, Hugh. "Feeling the heat from employees, Wall Street banks get closer to adopting bitcoin" CNBC (Feb. 12, 2021). https://www.cnbc.com/2021/02/12/bitcoin-banks-closer-accepting-cryptocurrency-asset-class.html

[6] Rooney, Kate. "Square and PayPal may be the new whales in the crypto market as clients flock to buy bitcoin" CNBC (Nov. 24, 2020). https://www.cnbc.com/2020/11/24/square-and-paypal-emerge-as-whales-in-the-crypto-market-.html

[7] Bambrough, Billy. "Visa Reveals Bitcoin and Crypto Banking Roadmap Amid Race to Reach Network of 70 Million" Forbes (Feb. 3, 2021). https://www.forbes.com/sites/billybambrough/2021/02/03/visa-reveals-bitcoin-and-crypto-banking-roadmap-amid-race-to-reach-network-of-70-million/?sh=7cc0664b401c

[8] Fabian Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74. https://doi.org/10.20955/r.103.153-74 . See also, Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." 2013; https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[9] Financial Stability Board. "Crypto-asset markets: Potential channels for future financial stability implications" (Oct. 10, 2018). https://www.fsb.org/wp-content/uploads/P101018.pdf

of around $50 billion.[10] As we will discuss below, crypto markets are becoming highly interconnected with the traditional financial sector. In time, DeFi could become a significant, if not the predominant, type of financial system, platformizing to varying extents the traditional financial sector. In the meantime, we need to take on the challenge of identifying and assessing the unique features of DeFi and what risks DeFi pose to the financial system.

i. Evolution of DeFi Movement to DeFi

DeFi comprises several components and continues to evolve quickly: (1) the public base layer with the digitally native token, (2) software protocols that codify agreed rules, (3) smart contracts that implement financial logic (i.e., execute transactions once specific conditions are met), and (4) stablecoins backed by reserves held at banks. In this chapter, we look at the various components of the DeFi universe with a particular focus on software protocols (aka. DeFi/DeFi protocols). DeFi protocols are automated systems deployed on a public blockchain, typically Ethereum, whereby users can take advantage of liquidity supplied by many counterparties in order to engage in asset swaps or acquire leverage, without dealing with a centralized financial counterparty.

After a call for crypto regulation by France and Germany,[11] the G20 Ministers of Finance and Central Bank Governors instructed the Financial Stability Board (FSB) to assess its work and the work of standard-setting bodies on crypto-assets. The FSB concluded that crypto-assets "did not pose a material threat to global financial stability" at the time of assessment but that crypto-assets would require "vigilant" monitoring.[12][13] However, the FSB's approach focused on potential transmissions of risk to traditional financial sectors. We argue that, as DeFi becomes mainstream, regulators and industry will need to quickly get up to speed on how DeFi operates and what are its inherent risks for users and the real economy.

After the introduction in Section 1, Section 2 provides historical background on the evolution of DeFi. The main body of this chapter, Section 3, identifies and attempts to categorize DeFi risks into five main buckets. As we explore these crypto-centric risks, we keep in mind how these new risks compare to the traditional credit, liquidity, counterparty, market and operational risks, and how our understanding of these traditional risks could be applied to DeFi. How these traditional financial risks manifest themselves in DeFi may differ somewhat from traditional financial

---

[10] "Defi: Value Locked by category" The Block. Accessed April 12, 2021. https://www.theblockcrypto.com/data/decentralized-finance/total-value-locked-tvl

[11] https://www.telegraph.co.uk/technology/2018/02/09/france-germany-demand-bitcoin-clampdown/

[12] Financial Stability Board. "Crypto-asset markets: Potential channels for future financial stability implications" (Oct. 10, 2018). Accessed April 11, 2021. https://www.fsb.org/wp-content/uploads/P101018.pdf

[13] Financial Stability Board. "Crypto-assets: Report to the G20 on work by the FSB and standard-setting bodies" (16 July 2018). Accessed April 11, 2021. https://www.fsb.org/wp-content/uploads/P160718-1.pdf

sectors. Section 4 concludes and provides a preliminary analysis of what these crypto-based risks and vulnerabilities could mean to the global financial system.

2. Definitions

DeFi blockchain projects include decentralized exchanges (or "DEXs"), lending platforms where central intermediaries are not needed to hold funds and transactions occur on a peer-to-peer basis through automated processes,[14] and decentralized applications (or "dApps").[15] One definition of DeFi is "the movement that leverages decentralized networks to transform old financial products into trustless and transparent protocols that run without intermediaries."[16] Another defines DeFi to mean where it "expands the use of blockchain from simple value transfer to more complex financial use cases."[17] And as mentioned earlier, another more specific definition is "an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, such as the Ethereum blockchain."[18] Many argue that DeFi is a form of finance that uses blockchain and does not rely on traditional central intermediaries, such as banks, stock exchanges or broker/dealers.

DeFi has been rapidly evolving since the introduction of first generation bitcoin to the emergence of second generation stablecoins and the use of initial coin offerings (ICOs) to fundraise. These DeFi projects in theory can become active ecosystems, even alternatives to traditional financial systems, by leveraging smart contracts and decentralized asset custody to replace costly, traditional intermediaries.[19] Most DeFi projects are built on Ethereum, and many credit Ethereum's easy-to-program platform for enabling the explosion in DeFi projects. As of March 2021, 87% of 5,727 ICO-funded DeFi projects have been built on Ethereum.[20]

Researchers Chen and Bellavitis have identified four main categories of DeFi projects: (i) decentralized exchanges (DEXs), (ii) decentralized lending and borrowing, (iii) programmable decentralized derivatives, and (iv) automated financial processes.[21] Each of these categories

---

[14] *Supra*.
[15] See, https://ethereum.org/en/developers/docs/dapps/
[16] https://defiprime.com/
[17] Hertig, Alyssa. "What is DeFi?" Coindesk (Sept. 18, 2020, updated Dec. 17, 2020). https://www.coindesk.com/what-is-defi
[18] Schär (2021), supra.
[19] Qian, DJ. "Defi's Rise is Inevitable, and Fusion is Driving this Evolution of Conventional Finance" Bitcoin.com (Aug. 10, 2020). https://news.bitcoin.com/defis-riseDefi's Rise Is Inevitable, and Fusion Is Driving This Evolution of Conventional Finance – Sponsored Bitcoin News-is-inevitable-and-fusion-is-driving-this-evolution-of-conventional-finance/
[20] www.icobench.com. Accessed March 1, 2021.
[21] Chen, Yan & Bellavitis, Cristiano. (2020). "Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models." Journal of Business Venturing Insights 13 (June 2020). 10.1016/j.jbvi.2019.e00151.

possesses a set of risks, but they share some common features. They all leverage decentralized infrastructure and smart contracts. Smart contracts, however, are not legal contracts. They are software protocols that live "on chain" to automatically implement a procedure, legal contract or business practice.[22]

Why use smart contracts? Why use DeFi at all? The benefits of automated delivery of financial services by smart contracts are attractive. The transparency offered by blockchain technology provides efficient auditing of solvency and proof of reserve. Decentralization and the process of unbundling financial services can remove expensive traditional intermediaries – making finance more equitable. The use of smart contracts can also reduce execution risk. DeFi could allow for more open and cheaper access to financial services, reducing costs and risks from using centralized intermediaries. DeFi also holds the promise of interoperability across blockchains. This borderlessness of DeFi can help tear down financial sector silos, greatly promoting innovation and building vibrant financial ecosystems.

DeFi is not without its challenges, though. It introduces new types of risks, discussed below in Section 3. The promise of interoperability offered by DeFi has led to a concentration of nearly all DeFi projects on the blockchain Ethereum - a new form of concentration risk. Ironically, in the mission to remove humans and automate as much as possible, other risks have been either introduced or amplified, including the challenge to maintain code security. The growth of DeFi will also depend on its ability to navigate and build compatibility with traditional finance. It will also depend on how national and state laws and regulations evolve. Perhaps the biggest challenge of all is that the DeFi ecosystem continues to grow while its underlying base layer (public infrastructure such as Bitcoin or Ethereum) faces growing pains, manifesting in high fees.

3. Risk Factors in DeFi

The DeFi system is predicated on the notion of extreme transparency in which anyone can effectively see everyone else's transactions (although larger entities have found ways to be anonymous by using popular analytics tools, such as pseudonymity and privacy enhancing features). Extreme transparency offers tremendous potential for disintermediating traditional financial intermediaries and automating delivery of financial services. But extreme transparency also provides ample opportunities for exploitation. At its core, DeFi depends on shared, public databases with public read access and unfettered write access – provided the entity adding an

https://www.researchgate.net/publication/337111343_Blockchain_Disruption_and_Decentralized_Finance_The_Rise_of_Decentralized_Business_Models

[22] See definition: "'Smart contracts' is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform." https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

entry in the blockchain pays a sufficient fee. Anyone with knowledge of these systems, an internet connection, and sufficient tokens to pay for fees can deploy a smart contract that any other user can subsequently engage with in a permissionless manner. Smart contracts are software protocols that live "on-chain" – they are publicly available for anyone to engage with, audit, or scrutinize. This open access to smart contracts vastly increases the scope for financial innovation, as developers, for instance, are not limited by financial institutions requiring permission to engage with their APIs. Inevitably, this also introduces new forms of risk, as there are no required professional or licensing qualifications restricting who can deploy, manage, or engage with smart contracts.

A general objective shared by DeFi practitioners is stripping human discretion from financial contracts, and encoding the rules for behavior into highly automated, publicly available systems. In practice, however, human discretion remains. DeFi systems must be deployed, governed, and upgraded, and face occasional bugs or exploitative interactions with other protocols. They also run on public blockchains, which face similar issues – and occasionally require human intervention, too. As such, the core DeFi protocols tend to retain some level of human involvement from controlling entities. This is a means to mitigate risks when they emerge, but it also poses a potential threat to these systems if the administrators themselves are compromised, malicious, or somehow co-opted.

Some risk factors and exploits are analogous to those evident in existing financial products, like market risk, the manipulation of an underlying price to interfere with a derivative – one of the most frequent forms of attack against DeFi protocols, and frontrunning transactions through fee upping and quant models. Others are completely novel and idiosyncratic to the asset class, like protocol-level reorganizations to invalidate prior transactions, validators reordering transactions to extract value from on-chain marketplaces, or 'flash loans' giving attackers unlimited free leverage.[23]

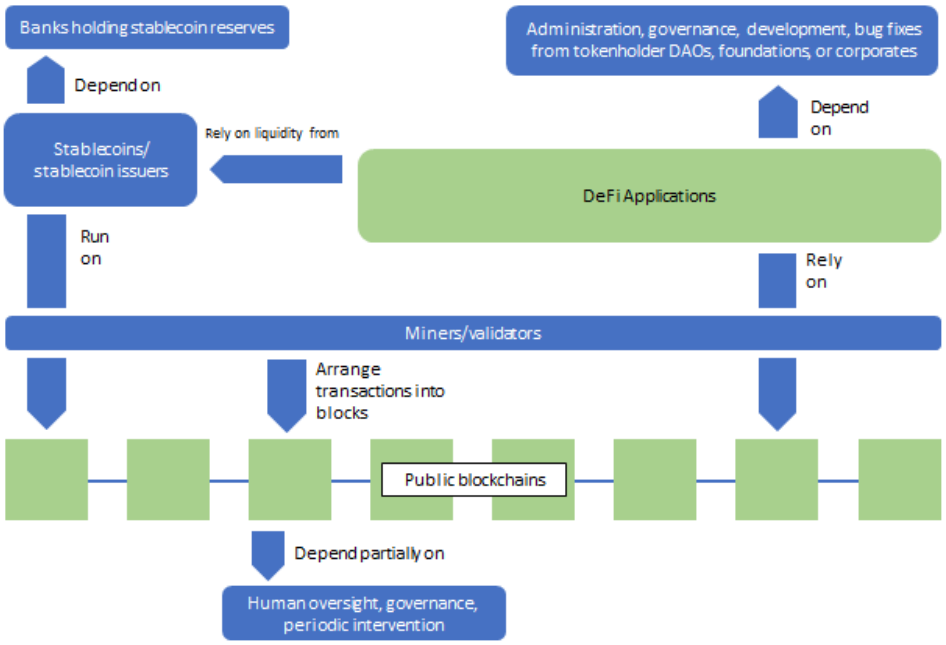
We divide our discussion of DeFi risk factors into five general buckets:

(i) interconnections with the traditional financial system,
(ii) operational risks stemming from underlying blockchains,
(iii) smart contract-based vulnerabilities,
(iv) other governance and regulatory risks, and
(v) scalability challenges.

[23] There has been a series of flash loan attacks in the past year. Most recently as of time of writing, PancakeSwap, a yield-farming aggregate (value lostunknown) and bEarn.Fi, a cross-chain farming protocol (loss of almost $11 million) suffered flash loan attacks. See, Crawley, Jamie "Flash Loan Attack Causes DeFi Token Bunny to Crash Over 95%" CoinDesk (May 20, 2021). https://www.coindesk.com/flash-loan-attack-bunny-token

The list of risks identified in this chapter is by no means exhaustive, but we attempt to outline the primary categories.

Figure 1. DeFi Protocols: Map of Interconnected Risks



Note: DeFi applications (e.g., MakerDao) rely on public blockchains (e.g., Ethereum, Bitcoin), which in turn rely on miners/validators to validate blocks of transactions as well as human oversight and governance. DeFi protocols are subject to governance, administration and maintenance. They rely on liquidity from stablecoins backed by reserves held at banks. (Green: decentralized, blockchain-based. Blue: centralized)

i. Interconnections with traditional financial system

a. Banks holding reserves backing stablecoins

While DeFi aspires to create a parallel and independent financial system based on code rather than legal enforcement, key components of the DeFi system rely in practice on traditional financial market infrastructure. The most critical nexus between the two systems can be found in stablecoins. These consist of dollar-denominated tokens circulating on public blockchains and, in principle, are backed by commercial bank dollars immobilized at financial institutions.

Stablecoins are useful for transactions in DeFi as they introduce fiat-denominated collateral into the open transactional context[24] of public blockchains. However, the vast majority of stablecoins derive their value from underlying dollar instruments and thus introduce a dependency on an issuer of the underlying instruments and the financial institution where the dollars are parked. At the time of writing, at least $65 billion worth of stablecoins circulate on public blockchains, but only around $3.1 billion consists of non-redeemable stablecoins issued against crypto-native collateral.[25] The remainder is fully dependent on an ongoing bank relationship and the promise of redeemability for the underlying instruments to be upheld.

Even some of the most purportedly decentralized stablecoins have introduced points of compromise. The MakerDAO system is a set of tools for issuing dollar-denominated tokens (named "Dai", which is "soft-pegged" to the US dollar[26]) in an automated way against an overcollateralized basket of other assets. Issuing dollar-denominated assets against crypto collateral within a smart contract is intended to insulate the token from the traditional financial system and potential points of compromise.

i. Market risk in stablecoins' underlying collateral

In November 2019, MakerDAO introduced "non-native" forms of collateral backing the Dai to manage market volatility of ether (ETH).[27] Initially, all Dai were issued in an overcollateralized manner against the digitally-native cryptocurrency ether. Collateralizing against ether made the MakerDAO system more insulated from third-party liabilities, less interdependent with traditional finance and, thus, arguably more robust and resilient. Since ether is no one's liability and its value is solely market-determined, it is arguably more suitable to back assets like Dai as long as its downside volatility is managed.

However, in November 2019, Maker diversified the portfolio of crypto-assets backing Dai in order to obtain a less volatile collateral, including the USD Coin (USDC), Tether (USDT), Wrapped Bitcoin (WBTC), and Basic Attention Token (BAT).[28] This collateral diversification introduced new risks. These new collateral types were not "liability-free" like ether, but in some cases the liability of a single issuer. As of the time of writing, $1.06 billion worth, or 16 percent,

[24] 'Open transactional context' means public blockchain-based assets can be exchanged on a peer-to-peer basis worldwide with virtually no oversight. In practice, most stablecoin transactions happen on the internals of the transactional graph and do not involve the issuer (and are hence not exposed to KYC/AML). Keep in mind that most stablecoins refer to the USD as their unit of account, but others target alternative sovereign currencies.

[25] Coinmetrics, Dai and sUSD as the crypto-native stablecoins in question. Data current as of Apr. 12, 2021.

[26] "Busting MakerDAO Myths: Seven Misconceptions about Dai" (Nov. 11, 2020). https://blog.makerdao.com/busting-makerdao-myths-seven-misconceptions-about-dai/

[27] *Id*.

[28] https://daistats.com/#/

of the $6.5 billion collateral in the MakerDAO system represents the liability of a third party.[29] All of the assets in question can be frozen by entities administering these stablecoin systems, obviating the trustlessness of a portion of the MakerDAO system. For example, if the USDC governing consortium Centre were to freeze the $332 million worth of USDC[30] held in the MakerDAO reserve, MakerDAO's ability to maintain the dollar peg of Dai could be compromised. Furthermore, while Centre's USDC has largely coexisted with DeFi, this status quo could be tested should a regulator apply pressure to Centre[31] (primarily the founding members Circle or Coinbase) or the regulated financial institutions issuing USDC. Centre's blacklisting policy indicates that they would blacklist blockchain addresses in order "[t]o comply with a law, regulation, or legal order from a duly recognized US authorized authority, US court of competent jurisdiction, or other governmental authority with jurisdiction over Centre."[32] Additionally, the banks holding reserves backing USDC could withdraw their support for the token issuer, as happened repeatedly with the stablecoin Tether.[33] [34] So the presence of liability-laden collateral in purportedly purely crypto-economic systems like Maker/Dai injects the potential for interference through regulatory oversight, commercial bank policy, or direct action from the stablecoin issuer itself.

ii. Sources of market illiquidity

As for the standard fiat-backed stablecoins, they now account for a significant share of liquidity for the major DeFi protocols. The top five DeFi protocols by USD-equivalent amount of collateral supplied – MakerDAO, Curve, Uniswap, Aave, and Compound – collectively host

---

[29] The assets in question included 'wrapped BTC', and the stablecoins USDC, USDT, GUSD, Paxos, TUSD. Data current as of Apr. 12, 2021.

[30] https://duneanalytics.com/hagaetc/maker-dao---mcd. Figures current as of Mar. 15, 2021

[31] For example, the FATF may consider centralized stablecoin issuers to be Virtual Asset Service Providers (VASPs) and has suggested in their draft March 2021 guidance that member states impose additional disclosure burdens on VASPs facilitating 'unhosted' transactions (possibly capturing how stablecoin issuers operate). See p. 71, "Draft updated Guidance for a risk-based approach to virtual assets and VASPs" FATF (March 2021). https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf

[32] https://f.hubspotusercontent30.net/hubfs/9304636/PDF/Centre_Blacklisting_Policy_20200512.pdf

[33] See, Attorney General of the State of New York. "Settlement agreement with Tether and Bitfinance" (July 2020). https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf

[34] Tether is a controversial so-called stablecoin that was unable to substantiate its dollar reserves. Despite the unclear backing of its dollar reserves. Nonetheless, Tether is an important source of liquidity in crypto-finance. See, Attorney General's settlement with Tether (2020), *supra*. To comply with this settlement, Tether released for the first time in May 2021 a breakdown of its reserves composition. As of March 31, 2021, Tether's reserves were composed of 75.85% cash and equivalents, 12.55% secured loans, 9.96% in corporate bonds and precious metals and 1.64% in other investments, including digital currencies. Interestingly, 49% is backed by unspecified commercial paper. See, De, Nikhilesh. "Tether's First Reserve Breakdown Shows Token 49% Backed By Unspecified Commercial Paper" CoinDesk (May 13, 2021). https://www.coindesk.com/tether-first-reserve-composition-report-usdt

$3.818 billion in USDC and $1.06 billion in Tether (USDT) in deposits.[35] These figures represent 42 percent of outstanding USDC and 5.2 percent of outstanding USDT circulating on Ethereum.[36] These two stablecoins represent critical sources of liquidity for these various DeFi protocols. USDC represents 19.5 percent of collateral on the lending protocol Compound, and the USDC-ETH pair is the second-most liquid pair on the decentralized exchange Uniswap. These stablecoins are naturally exposed to the failure of the banks holding collateral reserves backing these two stablecoins. Historically, banking support for certain stablecoin issuers can be questionable, as evidenced by the disclosures found in a settlement agreement between Tether and the New York Attorney General's office.[37] A bank insolvency, regulatory action, or issuer failure – likely causing the stablecoins in question to trade at a discount to par, as happened historically during confidence crises[38] – would impair the collateral and liquidity that powers these DeFi systems.

b. High interconnectedness: banking relationships with crypto trading firms

Aside from stablecoin banking, a handful of banks provide critical services to cryptocurrency firms. Historically, only a small number of U.S. banks, including Silvergate Bank, Signature Bank, and Metropolitan Community Bank, have actively pursued clients in the DeFi space. These banks represent critical points of centralization for the crypto industry. A disruption or an insolvency among any one of these banks would adversely affect whole swathes of the cryptocurrency industry.

Perhaps the bank with the greatest concentration of the crypto industry, Silvergate Bank is a California state-chartered bank based in San Diego that turned its focus to the cryptocurrency industry in 2013 and now provides banking services to firms active in this space. Their flagship product is the Silvergate Exchange Network (SEN), which enables real-time USD transfer between its clients, which are largely centralized crypto exchanges and institutional investors.[39] Acquiring banking services has been so challenging for crypto exchanges and firms that

---

[35] Maker: https://duneanalytics.com/hagaetc/maker-dao---mcd, Curve https://www.curve.fi/totaldeposits, Uniswap https://info.uniswap.org/home, Aave https://aavewatch.com/ , Compound https://compound.finance/markets (As of March 15, 2021)

[36] Based on figures: 9 billion USDC circulating and 20.41 billion USDT_eth circulating (Source: Coin Metrics). (As of March 15, 2021)

[37] NY Attorney General Letitia James. Press Release: "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York" (Feb. 23, 2021). https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal

[38] For instance, when Wells Fargo withdrew its support for Tether in spring 2017 and convertibility was temporarily suspended, (https://bitcoinist.com/bitcoin-trading-at-a-premium-on-bitfinex-and-poloniex/) Tether traded as low as 92 cents on the dollar (Coin Metrics data)

[39] Silvergate Capital Corporation Investor Presentation (January 2021). https://s23.q4cdn.com/615058218/files/doc_presentations/2021/01/Silvergate-Capital-Investor-Presentation-January-2021.pdf

Silvergate has become a key nexus connecting traditional banking and the digital currency industry. As of 4Q2020, Silvergate boasted $5.5 billion in total assets on their balance sheet and $5.03 billion in cryptocurrency deposits.[40] Their SEN transfer network processed $59.2 billion in intra-bank transfer volume in the fourth quarter,[41] providing an alternative settlement means for crypto firms looking to settle the USD fiat leg of crypto-fiat trades. While a small number of more mature crypto firms are able to obtain banking relationships with the largest banks in the U.S.,[42] most firms active in the virtual currency industry rely on Silvergate and its peers, which are relatively small community banks, to settle the USD fiat leg of crypto-fiat trades and for banking services. Any instability or cessation of banking in this cohort could cripple the crypto industry, as crypto exchanges, brokerages, and OTC desks would have to scramble to find alternative sources of USD fiat liquidity. More recently, Facebook-backed Diem announced that Silvergate will be the exclusive issuer of the Diem USD stablecoin in a sudden about-face from a cross-border payments strategy to a US-centric approach.[43] This partnership with Facebook's Diem only further augments the U.S. crypto industry's exposure to Silvergate.

c. Retail exposure: consumer fintech apps

DeFi has begun to cross the threshold to mainstream consumer fintech apps, thus moving beyond an audience of high-tech early adopters. A number of retail crypto exchanges have begun serving as interfaces for DeFi protocols, effectively reducing the frictions involved in getting access to DeFi – and exposing retail users to their benefits and risks. Now there are publicly traded firms that depend on the functionality of smart contracts and may well have user funds deposited with them.

Consumer fintech apps now make crypto highly accessible to retail investors who may not fully understand what they are trading. The popular retail-facing brokerage Coinbase, which boasts 56 million verified users as of their Q1 2021 quarterly filing,[44] has begun to embrace DeFi, positioning themselves among other things as an interface to these blockchain protocols. For instance, Coinbase details their growing proximity to and engagement with the decentralized interest rate swap protocol Compound in its Form S-1:

---

[40] Silvergate Capital Corporation 4Q20 Earnings Presentation (Jan. 20, 2021). https://s23.q4cdn.com/615058218/files/doc_financials/2020/q4/Ex.-99.2-SI-4Q20-Earnings-Presentation-1.20.2021.pdf

[41] Silverage SEN Network Transfer Volume (Quarterly) Q42018 - Q4 2020. https://www.theblockcrypto.com/data/crypto-markets/public-companies/sen-transfer-volume

[42] Palmer, Daniel. "JPMorgan Bank Takes on Coinbase, Gemini as Its First Crypto Exchange Customers" Coindesk (May 12, 2020). https://www.coindesk.com/coinbase-gemini-first-crypto-exchange-customers-jpmorgan-bank-report

[43] Diem Association. "Partnership with Silvergate and Strategic Shift to the United States" (May 12, 2021). https://www.diem.com/en-us/updates/diem-silvergate-partnership/

[44] Coinbase First Quarter 2021 Announcement. https://investor.coinbase.com/news/news-details/2021/Coinbase-Announces-First-Quarter-2021-Estimated-Results-and-Full-Year-2021-Outlook/default.aspx

> *Our relationship with Compound began in 2018 when Coinbase Ventures invested in Compound Labs, Inc., the DeFi pioneer behind the Compound protocol. Coinbase was also an early adopter of Compound, supplying USDC liquidity to the protocol in 2019 and allowing Coinbase Wallet users to access Compound directly starting in early 2020.*[45]

A number of other cryptocurrency brokers, custodians, and lenders have begun to see themselves as interfaces to DeFi protocols, in addition to their core businesses.

Binance, one of the largest spot and derivatives exchanges for cryptocurrencies, has reported a 24 hour trading volume of $80 billion on January 4, 2021[46] and has over 350,000 BTC and 3.6 million ETH held on deposit on behalf of clients.[47] This large cryptocurrency exchange has now openly embraced DeFi, providing not only a centralized brokerage and exchange experience, but a number of passthrough products enabling users to participate in decentralized protocols through its Binance Earn[48] suite.

Additionally, the Swiss fintech firm Taurus Group has integrated the lending and borrowing Aave protocol[49] into its infrastructure, permitting institutional clients to access liquidity on the DeFi protocol.[50] This presages a possible scenario where fintechs or financial institutions start to put client assets in DeFi protocols in order to take advantage of attractive interest rates,[51] which are generally higher than returns on cash held at banks (although they offer fundamentally different risk profiles).

d. Corporate exposure: corporate treasuries

Lastly, some corporations are obtaining direct exposures to native cryptocurrencies on their balance sheet, either as an alternative treasury asset (as with Microstrategy, Square, or Tesla) or

---

[45] Coinbase Global, Inc. Form S1 Registration Statement. (filed with the SEC on Feb. 25, 2021). https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm

[46] Binance reported daily trading volume of $80 billion in 24-hour trade activity on Jan. 4, 2021. See, Haig, Samuel. "Binance hits record high of $80B in daily volume as crypto markets surge" Cointelegraph (January 5, 2021). https://cointelegraph.com/news/binance-hits-record-high-of-80b-in-daily-volume-as-crypto-markets-surge

[47] CoinMetrics data. Data retrieved Mar. 15, 2021

[48] See, https://www.binance.com/en/earn#flex-item

[49] Aave is a "decentralised non-custodial liquidity market protocol" in which users can provide liquidity to earn an interest rate, or borrow against their assets in either an overcollateralized manner or undercollateralized with a flash loan. https://docs.aave.com/faq/

[50] Akhtar, Tanzeel. "Digital Assets Firm Taurus Integrates Aave Protocol to Improve Banking Access to DeFi" Coindesk (Mar. 8, 2021). https://www.coindesk.com/digital-assets-firm-taurus-banking-access-defi-aave-partnership

[51] See, https://defirate.com/lend/

in preparation to actually use the tokens to transact on the protocol directly. This presages more engagement from public corporations with these shared infrastructures. The Chinese smartphone firm Meitu Inc. acquired 15,000 ETH (worth $22m at the time of purchase), citing its potential utility in future transactions on the Ethereum network:

> *[T]he Ether purchased would become the gas reserve for the Group's potential dAPP(s) to consume in the future, as well as being used as consideration for investing in blockchain-based projects that take Ether as consideration.*[52]

Meitu indicated in their disclosure that they were considering launching Ethereum-based dApps, and would thus require a reserve of ether in order to transact on the Ethereum network.

While interactions between traditional firms and DeFi systems have been historically sparse, growing evidence suggests that integration is taking place. The earliest adopters were crypto exchanges exchanging crypto-assets with traditional assets and providing passthrough services to DeFi protocols. More interactions are emerging between banks servicing crypto businesses, transacting on these networks directly and increasingly with other firms looking to benefit from the assurances of public blockchains. More recently, Visa announced their intention to engage with DeFi directly, enabling the settlement of transactions with USDC on the Ethereum network.[53] As DeFi comes to offer more modes of transactions, firms like Meitu may come to have an interest in using these DeFi networks directly. Such corporate firms will need to assess their risk exposures to a protocol's smart contracts and underlying cryptocurrency and blockchain (discussed below). They will also need to assess how they may even pass these risks on to their customers and business partners.

ii. Operational risks stemming from underlying blockchains

DeFi applications ultimately rely on public blockchains for settlement and contract resolution. The most popular base layer, as measured by liquidity for such applications, is Ethereum with around $46 billion worth of collateral (composed of various crypto-assets and stablecoins) being employed in Ethereum-based smart contracts.[54] A number of other blockchains now host DeFi applications and are eyeing Ethereum's lead.

---

[52] Meitu, Inc. Voluntary Announcement: Purchase of Cryptocurrencies (Ether and Bitcoin) (Mar. 7, 2021). (https://corp-static.meitu.com/corp-new/92016878a68bac4ad8121e906eae6687_1615115628.pdf

[53] Visa. "Digital currency comes to Visa's settlement platform." (Mar. 29, 2021). https://usa.visa.com/visa-everywhere/blog/bdp/2021/03/26/digital-currency-comes-1616782388876.html

[54] Gross Value Locked and Net Value Locked (Ethereum DeFi). Accessed April 12, 2021. https://www.theblockcrypto.com/data/decentralized-finance/total-value-locked-tvl/true-value-locked-and-total-value-locked

The orderly operation of these applications relies critically on these base layer blockchains functioning, which cannot always be guaranteed. Transacting parties internalize novel risks, which may have no analogues in traditional finance where messaging and settlement systems are governed by single entities or bodies (like SWIFT, The Clearing House, or the Federal Reserve with Fedwire). Instead, public blockchains are largely decentralized settings where validators are compensated for assembling transactions into blocks and are expected to do so honestly based on economic incentives.[55] As there are no central administrators in these systems, the responsibility for evaluating the risk of relying on these infrastructures effectively falls on the end users, applications, and new types of intermediaries involved in the DeFi systems.

a. Consensus failures

Consensus – the construction, approval and distribution of blocks of transaction across distributed ledgers – on these blockchains is, however, not a given. While the largest and most robust blockchains such as Bitcoin and Ethereum experience virtually no outages, outages are not completely unheard of. Bitcoin infamously had two major "rollbacks" in 2010[56] and 2013[57] when a significant number of blocks, and hence transactions, were unrecorded or essentially reversed. Collectively, around 15 hours' worth of transactions were removed over the course of those two events.

Ethereum is arguably more fragile to outages since most users do not run nodes but instead rely on service providers like Infura to query and index the blockchain and broadcast transactions. When these service providers experience downtime, as was the case with Infura during an unplanned chain split in 2020,[58] intermediated transactions ground to a halt.

b. Underlying protocol interventions

Blockchains are not immune to politics, as they are, after all, governed by the humans that establish their rules. Most infamously, in 2016, Ethereum leadership coordinated the selective removal of balances from the blockchain after a particularly large DeFi application called "The DAO" was hacked and exploited.[59] Ethereum leadership deemed it necessary to intervene on the

---

[55] For more reading about economic incentives, see, Auer, Raphael, Cyril Monnet and Hyun Song Shin. "Permissioned distributed ledgers and the governance of money" BIS Working Papers No 924 (January 2021). https://www.bis.org/publ/work924.pdf

[56] Coopahtroopa, Cooper. "YFI Minting Ownership" (Jul. 2020). https://gov.yearn.finance/t/yfi-minting-ownership/155

[57] Andresen, Gavin. "March 2013 Chain Fork Post-Mortem" (Mar. 3, 2020). https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

[58] Khalili, Joel. "Massive Ethereum outage forces crypto exchanges to block withdrawals" techradar.pro (Nov. 11, 2020). https://www.techradar.com/news/massive-ethereum-outage-forces-crypto-exchanges-to-block-withdrawals

[59] Siegel, David. "Understanding the Dao Attack" Coindesk (Jun. 25, 2016, updated Dec. 17, 2020). (https://www.coindesk.com/understanding-dao-hack-journalists

Ethereum blockchain due to the large fraction of outstanding ether locked in the faulty DAO contract. Some Ethereum community members rebelled against the arbitrary changes and supported the original Ethereum chain. The intervention caused a hard fork in the blockchain, as two versions of Ethereum came to exist in tandem (with the original, but less widely adopted, version ultimately being called "Ethereum Classic"). This is an example of a contract failure ultimately affecting the underlying protocol itself and demonstrating that certain critically large applications can take on a systemic nature within protocol politics. At the time of the exploit, The DAO contract accounted for 15 percent of ether outstanding at the time. While Ethereum leadership have not intervened to remediate subsequent hacks and failures, one might imagine that if a popular contract with a similar threshold of ether was breached, it might call them into action at the blockchain level once again. In the case of the DAO, Ethereum's future switch to Proof of Stake was cited as justification for rolling back the exploit (which would have granted a presumably hostile actor a large share of the outstanding ether, and hence a significant role in the future of the network under a Proof of Stake regime). Other less critical bugs or exploits have not met the seriousness threshold to merit a rollback, even when those affected lobbied Ethereum leadership.[60]

While the post-DAO hard fork of Ethereum is generally seen as a prudent move, it constituted, on strict terms, a violation of property rights and brought into question the settlement assurances of the blockchain. On Ethereum, there is no legal adjudication – knowledge of a private key is tantamount to ownership. Thus, under the protocol rules, the entity that exploited the DAO was the rightful owner of the ether in question, and those rules were overridden to "bail out" depositors in the DAO contract.[61] Such interventions could be helpful for obtaining recourse when catastrophic failures or bugs occur, but they also introduce subjectivity and arbitrariness into the settlement process.[62]

c. Proof of Work (PoW) consensus failures

[60] In the case of the Parity hack, Parity asked for (and were denied) a hard fork to undo the loss of 513k Ethere. See https://www.businessinsider.com/ethereum-price-parity-hack-bug-fork-2017-11

[61] Please note that holders of Ethereum Classic on the original blockchain kept their property rights but not the funds stolen in the DAO attack. Arruñada, Benito, Prospects of Blockchain in Contract and Property (February 23, 2020). See, Pompeu Fabra University, Economics and Business Working Paper 1696, 2020, Available at SSRN: https://ssrn.com/abstract=3543137 or http://dx.doi.org/10.2139/ssrn.3543137

[62] Settlement in the blockchain is a complex issue for blockchain systems and involves a combination of both operational and legal risks. In traditional finance, a number of operational and legal frictions are baked into the settlement process in both payments and trading,such as time, central intermediaries, and/or contractual agreements. These frictions, which also act as risk mitigation, do not often have analogous features on blockchains. Note also that the settlement process differs significantly between UTXO- vs account-based blockchains.

More straightforwardly, smaller blockchains can be exploited when miners believe they are not sufficiently compensated. When miners gain sufficient hashpower,[63] they can coordinate consensus attacks, of which a subset is known as reorganization attacks or "51 percent attacks". These attacks consist of exploits in which validators employ their privileged access to transaction ordering to extract some value from the blockchain. These consensus attacks generally take place on Proof of Work (PoW) blockchains because such blockchains provide relatively low compensation thresholds to miners, making validator attacks more economically plausible. Often, these attacks occur in the presence of general-purpose computing hardware, which can be borrowed or rented.[64]

As an example, in early 2021, validators on the Verge blockchain rolled back 200 days of data, effectively invalidating months of transactions.[65] These reorganizations of blocks can be used to omit certain transactions that were presumed settled, including deposits credited by an exchange. Thus, reorganizations are often tools for the fraudulently misleading merchants or crypto exchanges into believing that there is a valid deposit, which is then ultimately excluded from the ledger. Indeed, both the Ethereum Classic[66] and the Bitcoin Gold[67] blockchains have suffered multiple such protocol-level attacks, some of which were used to successfully defraud crypto exchanges. DeFi applications rely on the base layer blockchains to settle and clear transactions, so the application stack is compromised when the underlying blockchain malfunctions.

Both Ethereum and Bitcoin currently rely on PoW, so they are theoretically exposed to these kinds of attacks. However, Ethereum and Bitcoin offer incredibly large security budgets,[68] making an attack extremely expensive and likely impractical. Additionally, Bitcoin is mined with bitcoin-focused hardware (known as "Application-Specific Integrated Circuits" or ASICs) that cannot be repurposed for use in general computing or for most other crypto networks, so miners would have less incentive to attack the Bitcoin blockchain and destroy what gives their Bitcoin ASICs value. Moreover, as Bitcoin ASICs are essentially the physical embodiment of future cash

[63] "Hashpower" of "hashrate" refers to "the total combined computational power that is being used to mine and process transactions on a Proof-of-Work blockchain, such as Bitcoin and Ethereum (prior to the 2.0 upgrade)." See, https://www.coindesk.com/what-does-hashrate-mean

[64] Note: a 51% attack allows malicious actors to unrecord or prevent the recording of transactions, but not to fraudulently generate new transactions that they cannot otherwise digitally sign. Of course, ordering and recording of blocks can be powerful tools nonetheless, particularly for crypto-finance.

[65] Mapperson, Joshua. "Verge of disaster: 200 days transactions wiped from blockchain," Cointelegraph (Feb. 16, 2021). https://cointelegraph.com/news/verge-of-disaster-200-days-transactions-wiped-from-blockchain

[66] Shen, Muyao. "Crypto Investors Have Ignored Three Straight 51% Attacks on ETC," Coindesk (Sept. 8, 2020). https://www.coindesk.com/crypto-51-attacks-etc

[67] Nelson, Danny. "Attempted 51% Attack on Bitcoin Gold Was Thwarted, Developers Say" Coindesk (Jul. 10, 2020). https://www.coindesk.com/attempted-51-attack-on-bitcoin-gold-was-thwarted-developers-say

[68] On a trailing seven day basis, Bitcoin offers miners an average of $60m/day, and Ethereum is offering miners $48m/day (Source: Coin Metrics, as of Apr. 12, 2021).

flows in bitcoin over the ASIC's useful lifetime, miners are strongly incentivized to support the long term value of the Bitcoin blockchain.[69]

Similarly, a large share of the value of the high-end graphics processing units (GPUs) used to mine ether derives from the value of ether itself,[70] so miners attacking the Ethereum blockchain would be depreciating their own equipment in doing so. For blockchains such as Bitcoin with a capped issuance, questions remain over the long run viability of PoW when Bitcoin becomes a network based solely on transaction fees. Various studies have identified the potential instability or insufficiency of a fee-based PoW market environment.[71]

d. Miner extractable value (MEV)

Nevertheless, reorganizations of blocks (or 51 percent attacks) are only one class of a broader set of validator-based exploitations known as "miner extractable value" (or MEV).[72] First introduced by researchers Daian et al (2019),[73] the term MEV refers to the value that validators (the entities assembling transactions into blocks) or third parties can extract from transacting users by frontrunning them and selectively reordering transactions.[74] MEV is made possible due to the innate transparency of Ethereum transactions, their utility in on-chain exchanges, and the possibility of gaining priority by outbidding other users (or simply reordering transactions if you are the miner). MEV can be thought of as somewhat analogous to a hedge fund paying for order flow in order to trade against uninformed or retail flow.

---

[69] Note: there could be a risk of state action. For example, Chinese authorities could take control of a significant chunk of bitcoin mining. https://blog.lopp.net/are-chinese-miners-threat-bitcoin/

[70] It is helpful to think of the hardware used to mine blockchains as a physically-instantiated bundle of call options for the underlying token gradually unlocking over the useful lifetime of the hardware.

[71] See, Carlsten, Miles & Harry Kalodner, Matt Weinberg, and Arvind Narayanan. Working Paper: "On the instability of Bitcoin without the block reward." PrincetonEconomics (Oct. 2016). https://economics.princeton.edu/working-papers/on-the-instability-of-bitcoin-without-the-block-reward/. See also, Budish, Eric. "The Economic Limits of Bitcoin and the Blockchain" University of Chicago Booth School of Business,(Jun. 5, 2018) https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf, and Auer, Raphael. "The doomsday economics of 'proof-of-work' in cryptocurrencies" VOXeu/CEPR (Mar. 8, 2019). https://voxeu.org/article/doomsday-economics-proof-work-cryptocurrencies

[72] Because not all entities extracting value in this manner are miners, MEV is sometimes styled as "Maximal Extracted Value"

[73] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges" (Apr. 10, 2019). https://arxiv.org/abs/1904.05234

[74] Flashbots defines MEV as "the total value that can be extracted permissionlessly (i.e. without any special rights) from the re-ordering, insertion or censorship of transactions within a block being produced. As miners currently have the ultimate say on transaction ordering and inclusion in Ethereum, they can be seen as the most powerful player in this game [...] MEV exists on any blockchain and layers where there is a party responsible for transaction ordering (eg. validators, rollup providers)." Flashbots.net, "FAQ". Accessed Apr. 13, 2021. https://explore.flashbots.net/faq

As the complexity of transactions increases, more frontrunning and risk-free arbitrage opportunities emerge. Thus, the vast majority of observed MEV takes place on Ethereum, and largely relates to transactions occurring on automated market maker (AMM) exchanges – where users can frictionlessly swap assets by engaging with pools of liquidity. AMMs offer users guaranteed liquidity on exchanges, albeit at the potential cost of efficient execution. According to Flashbots.net, a lower bound of $369 million worth of MEV has been harvested by validators (or arbitrage bots) since January 2020.[75] This represents a net drag on users, which end up financing the MEV through slippage on their trades. Effectively, MEV can be understood as similar to a rake at a casino.

Most researchers consider MEV endemic to blockchains – like Ethereum – where transactions on decentralized exchanges or DEXs (including DEX platforms employing Automated Market Makers, such as Uniswap) are transparent. If the parties engaged in frontrunning materially degrade users' transactional experience, the logic of transparent DeFi could be called into question. While some analysts contend that MEV represents an alternative subsidy to miners or validators,[76] permitting blockchains to function at a lower level of issuance or fees, researchers Qin, Zhou and Gervais have highlighted how aggressive MEV poses a threat to consensus. In their estimate, "[the] biggest danger lies in the willingness of miners to extract and compete over MEV, which would increase the stale block rate and consequently aggravate the risks of double-spending and selfish mining."[77] Stale blocks and double spending reduce the predictability of the base layer and introduce uncertainty into settlement finality, impairing the assurances of crypto-economic protocols.

In an attempt to mitigate the protocol-level harms of MEV, Ethereum developers have proposed an Ethereum node client that codifies MEV and allows miners to auction off their rights to reorder transactions within a block, delegating the process of finding risk-free arbitrage to specialized third parties.[78] This would turn MEV into an explicit part of the compensation structure for miners, reduce the protocol instability caused by the current adversarial state of MEV, and increase fairness in mining by allowing less sophisticated miners to cheaply monetize MEV. Other researchers, unconvinced by the codification of MEV, have proposed alternative solutions, such as fair transaction ordering, or the encryption of transactions between the

[75] https://explore.flashbots.net/. Accessed Apr. 12, 2021.
[76] As of Apr. 12, 2021, 58 percent of Ethereum hashrate is associated with pools auctioning off the rights to reorder transactions via the Flashbots protocol. Effectively, these miners are selling the rights to specialists who extract economic rent by engaging in frontrunning trades. See, Flashbots Transparency Report - March 2021 (Apr 12). https://medium.com/flashbots/flashbots-transparency-report-march-2021-d3930b4b98a9
[77] Qin, K., Zhou, L., and Gervais, A. "Quantifying Blockchain Extractable Value: How dark is the forest?" (Jan. 22, 2021). arXiv.2101.055==v3 [cs.CR] 22 Jan 2021 https://arxiv.org/pdf/2101.05511.pdf
[78] See, Floersch, Karl. "MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value" ethresear.ch (Jan. 2020). https://ethresear.ch/t/mev-auction-auctioning-transaction-ordering-rights-as-a-solution-to-miner-extractable-value/6788 and https://ethresear.ch/t/flashbots-frontrunning-the-mev-crisis/8251/1

broadcast and execution stage.[79] Due to the downsides associated with broadcasting transactions to a global mempool,[80] privately-mined transactions are becoming more popular. Effectively, this involves routing transactional data to miners directly in a manner reminiscent of dark pools. At the time of writing, over 75,000 Ethereum transactions have been sent directly to miners[81] rather than being broadcast to the network in the conventional manner.

At present, MEV appears to be a fundamental feature of data-rich blockchains that facilitate transparent on-chain exchange. Transparent queuing systems for pending transactions combined with the ability to outbid and displace a transaction inevitably yields exploitation opportunities. Unlike a retail brokerage like Robinhood selling customer order flow,[82] MEV extractors are not obliged to the individuals they are arbitraging. Thus, there are no natural limits to the exploitation of end users through MEV.

e. Validator Cartels

Non-PoW blockchains are not immune to protocol interventions at the validator level. One popular alternative to PoW is known as Proof of Stake, where the power to assemble transactions into blocks (and, in some cases, exert political power over the network) is a function of one's share of all protocol tokens held. In certain network arrangements, the number of validator slots is fixed, creating strong incentives to consolidate power and cartelize. Because validators are typically rewarded with fees or new issuance, the consolidation of power through vote-buying has been observed[83] in Proof of Stake blockchains, such as EOS (which maintains 21 slots for validators). Such measures allow validators to consolidate power, granting them eventual control over which transactions can be included in the final ledger. If validators are fixed and free market competition for blockspace is snuffed out, the censor-resistance of the protocol properties would be at risk. Since DeFi is built on the assumption that the underlying financial infrastructure is neutral and unstoppable, such concentration of power in validators is a significant threat. An instance of validator collusion can be found on the STEEM network, where STEEM coins owned by blockchain entrepreneur Justin Sun were frozen after validators suspected his intentions to co-opt the network:

---

[79] Juels, Eyal, and Kelkar. "Miners, Front-Running-as-a-Service Is Theft," Coindesk (Apr. 7, 2021). https://www.coindesk.com/miners-front-running-service-theft

[80] The memory pool or mempool is a node's holding area for broadcasted but un-mined transactions. Transactions present in the mempool are transparent to anyone participating in consensus.

[81] Etherscan, "Private Transactions." Data current as of Apr. 14, 2021. https://etherscan.io/txs/label/private-transaction

[82] See, Roberts, Jeff John and Morris, David. Robinhood makes millions selling your stock trades … is that so wrong?" Fortune (July 8, 2020). https://fortune.com/2020/07/08/robinhood-makes-millions-selling-your-stock-trades-is-that-so-wrong/

[83] Dale, Brady. "EOS investors can't say they weren't warned." Coindesk (Oct. 3, 2018). https://www.coindesk.com/vitalik-called-it-vote-buying-scandal-stokes-fears-of-eos-failure

> *Specifically, the witnesses were able to unilaterally lock out Sun after a simple majority vote passed 19 to 1. They had orchestrated the plan in a private Slack group, ran a software upgrade on the blockchain and froze the Tron Foundation CEO's funds.*[84]

In this case, Sun fought back by enlisting custodial exchanges – which held large fractions of the supply of STEEM on behalf of users – to employ user deposits to vote in his favor and overrule the actions of the validators.[85] This illustrates how large cryptocurrency custodians and cryptocurrency deposit-taking institutions can take on vital roles as kingmakers in Proof of Stake systems. With Ethereum, the largest DeFi platform slated to transition to Proof of Stake, custodians holding large quantities of ether will have outsize control over the network and may be able to materially influence network outcomes. Thus far, crypto exchanges have generally not recused themselves from protocol interventions. Effectively, they act as principals rather than as agents when deploying client funds for on-chain votes.

f. Inflation bugs

Other more catastrophic protocol vulnerabilities abound, which can affect the DeFi applications built on top of them. One such risk is posed by inflation bugs, which inflate the supply of coins ahead of a pre-agreed or expected schedule.[86] As coins (minted in excess of the defined schedule) are issued and begin to circulate, recipients of these new coins have a strong disincentive to roll back the chain and undo the unexpected inflation. Inflation bugs are frequent and have affected many of the largest blockchain protocols – and in some cases, were not fully remediated. Blockchains that have witnessed material inflation bugs that were exploited include Bitcoin,[87] Bitcoin Private,[88] and Stellar,[89] as well as many other less notable cases.

---

[84] Copeland, Tim. "Steem vs Tron: The rebellion against a cryptocurrency empire" Decrypt (Aug. 18, 2020). https://decrypt.co/38050/steem-steemit-tron-justin-sun-cryptocurrency-war

[85] *Id*.

[86] Avan-Nomayo, Osato. "Inflation Bug Still a Danger to More than Half of All Bitcoin Full Nodes" Cointelegraph (May 19, 2019). https://cointelegraph.com/news/inflation-bug-still-a-danger-to-more-than-half-of-all-bitcoin-full-nodes

[87] See https://en.bitcoin.it/wiki/Value_overflow_incident

[88] CoinMetrics. "Don't Trust, Verify: a Bitcoin Private Case Study" Dec. 23, 2018. https://coinmetrics.io/bitcoin-private/

[89] Zmudzinski, Adrian. "Stellar Patched an Inflation Bug and Burned the Resulting 2.25 Billion XLM: Research" Cointelegraph (Mar. 27, 2019). https://cointelegraph.com/news/stellar-patched-an-inflation-bug-and-burned-the-resulting-225-billion-xlm-research

Other networks that have faced potential inflation bugs but were not known to have been exploited include Zcash[90] and Monero[91] – a particularly insidious threat when privacy-focused chains are concerned, as the inflation is harder to detect on more opaque blockchains. Another Bitcoin vulnerability patched in 2018[92] could have been used to create unexpected inflation but was not exploited. Since DeFi protocols are highly automated, run continuously, and operate with minimal (or in some cases, no) human oversight, inflation bugs on the underlying native protocols can significantly destabilize DeFi applications. Inflation bugs are among the most severe threats that blockchains face, and remediation often requires halting or rolling back the blockchain, which would impair the assurances of any smart contracts relying on the underlying blockchain. Recently, the DeFi-focused blockchain Kava was halted[93] to address a bug which was significantly overpaying planned distributions (known as 'yield farming').

iii. Smart contract-based risks

a. Technical vulnerabilities of smart contracts

Smart contracts as described earlier are not legal contracts. Instead, they are code that automates actions. These actions could be parts of native cryptocurrencies on public blockchains, such as bitcoin and ether, which can be understood as synthetic commodity money[94] – they are not guaranteed or backed by any third party and are not redeemable for anything, including fiat currency. Instead, they serve as 'access' tokens to the Bitcoin and Ethereum networks, respectively, and as a form of collateral and transactional medium within these networks.

For these native cryptocurrencies, it is fully possible to destroy, permanently immobilize, or render them unspendable. While some exploits (like the June 2016 DAO Hack on Ethereum[95] or the August 2010 Value Overflow Incident on Bitcoin[96]) represent such an existential threat to the

---

[90] Hackett, Rober. "Zcash Discloses Vulnerability That Could Have Allowed 'Infinite Counterfeit' Cryptocurrency" Fortune (Feb. 5, 2019). https://fortune.com/2019/02/05/zcash-vulnerability-cryptocurrency/

[91] Luigi1111 and Riccardo "fluffypony" Spagni. "Disclosure of a Major Bug in CryptoNote Based Currencies" Monero (May 17, 2017). https://www.getmonero.org/2017/05/17/disclosure-of-a-major-bug-in-cryptonote-based-currencies.html

[92] Hertig, Alyssa. "The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret" Coindesk (Sept. 21, 2018). https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret

[93] Harper, Colin. "Kava Halted After Yield Farming Bug Discovered in Latest Release" Coindesk (Mar. 4, 2021). https://www.coindesk.com/kava-halted-yield-farming-bug

[94] See, Selgin, George, Synthetic Commodity Money (April 10, 2013). Available at SSRN: https://ssrn.com/abstract=2000118 or http://dx.doi.org/10.2139/ssrn.2000118

[95] Siegel, Dan. "Understanding the Dao Attack" Coindesk (Jun 25, 2016). https://www.coindesk.com/understanding-dao-hack-journalists

[96] See, Value overflow incident. Accessed April 13, 2021. https://en.bitcoin.it/wiki/Value_overflow_incident

network that they have been remediated with recourse to social consensus (overriding the technical reality of the blockchain), the vast majority of exploits do not reach a critical threshold of importance. Therefore, users who interact with faulty smart contracts could risk losing all of their coins and are generally unable to obtain bailouts or recourse.

Perhaps the largest unremediated failure of a smart contract was the immobilization of 513,774 ether held in "multi-signature" ("multi-sig") wallets written by Parity,[97] an Ethereum development organization. Common multi-sig setups involve 2-of-3 or 3-of-5 schemes; the former would allow outputs to be spent if valid signatures from any two of three predetermined keys were provided.

The multi-sig wallets were exploited by an anonymous user who triggered a function in a smart contract, effectively causing each wallet to self-destruct, irredeemably immobilizing the ether contained within. The newly-locked ether – equivalent to 0.52% of all the ether in circulation at the time – was worth $174 million at the time of the hack and $1.175 billion at the time of writing.[98] Because Ethereum and other smart contract-enabled blockchains are more expressive[99] and permit more complex transactional logic, such failures are unavoidable. In this case, the faulty multi-sig wallets were produced by an organization run by Gavin Wood, one of the cofounders of Ethereum and the inventor of Solidity (Ethereum's dedicated programming language). The difficulty of writing a truly safe multi-sig contract illustrates the inherent risk involved in transacting with digital bearer assets on expressive – and hence, vulnerability-prone – base layers.

Moving beyond custodial risks, more complex interactions between smart contracts as required by DeFi protocols can introduce additional scope for potential vulnerabilities. DeFi is rife with purely technical vulnerabilities, owing to the complexity of interactive blockchain-based smart contracts and the difficulty of anticipating complete edge cases before deploying code. Smart contracts, once deployed, are cumbersome to upgrade, creating significant initial burdens on developers. In the case of certain irrevocable smart contracts - like Uniswap, developers have no ability to take down a smart contract once it is deployed. Upgrading such a smart contract would be a matter of deploying an alternative and persuading users to use it. As long as the underlying Ethereum blockchain remains intact, certain classes of smart contracts will remain operable regardless of administrator or user behavior. In certain other types of smart contracts, administrators can insert provisions into the code of their smart contracts so they can be upgraded, terminated, or deprecated. These code provisions grant developers additional discretion and recourse if there are bugs in deployed contracts. However, this has the externality

[97] Parity Technologies. "A Postmortem on the Parity Multi-Sig Library Self-Destruct" (Nov. 15, 2017). https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/

[98] Figures current as of April, 12, 2021

[99] The wider the set of computational concepts that can be expressed with base layer transactions the more expressive a blockchain is.

problems of potentially making administrators responsible for user funds as well as making the entities controlling the administrative keys a target for attackers.

Technical exploits are common: Werner et al (2021)[100] identified 21 such attacks on DeFi protocols between February to December 2020, costing users an aggregate of $144.3 million (USD value at the time of exploit) – although in some cases, funds were returned by attackers.

These exploits are varied in their approach, taking advantage of reentrancy bugs, "transaction sandwiches," logical bugs, and governance. In each case, however, attackers take advantage of the properties of DeFi: predictable algorithms managing large pools of capital with limited human oversight, built on blockchain rails. The rigidity of certain DeFi primitives, like Automated Market Makers, can facilitate many of these attacks. The natively on-chain nature of the collateral – in the case of ether – grants attackers the ability to withdraw their profits with no recourse. When the captured tokens include stablecoins or other assets that are the liability of a third party (such as exchange tokens), the tokens can be frozen.

b. Oracle attacks

One class of vulnerabilities deserving special attention relates to failures resulting from oracles. In DeFi, oracles are service providers that provide outside information to a smart contract. The most common usage of oracles is to transmit market prices, drawn from one or many exchanges, to a DeFi protocol that relies on outside pricing information. For example, protocols employing tokens as collateral would need to know the value (in standard terms like USD) of the pledged tokens and employ smart contracts that consume oracle-provided market information.[101]

A number of DeFi protocols rely on oracles, and the price inputs are critical to trigger liquidations, deleveraging, margin calls, and other forms of automated collateral management. Consequently, manipulation of oracles can be catastrophic for these protocols. It would be somewhat comparable to what would happen in traditional finance if Bloomberg were hacked and data were manipulated / could no longer be trusted.[102] Due to the sensitivity of these protocols to deviations between the spot price of an asset and an index price (opening up riskless arbitrage opportunities), so-called 'oracle attacks' are among the most popular means of attack. Similar to strategies that involve manipulating the spot reference price for a derivative, oracle attacks involve manipulating the market price of collateral referenced by a DeFi protocol in order to create riskless arbitrage or to trigger liquidations.

---

[100] Werner, S., Perez, D., Lewis, G., Klages-Mundt, A., Harz, D., and Knottenbelt, W. "SoK: Decentralized Finance (DeFi) arxiv.org (Mar. 2, 2021). arXiv:2101.08778v2 [cs.CR] 2 mar 2021 https://arxiv.org/pdf/2101.08778.pdf

[101] Note: oracle issues are not unique to crypto, but are harder to remediate because of transaction finality and lack of contractual priority among parties.

[102] See https://www.mas.gov.sg/-/media/MAS/resource/publications/fsr/FSR-2018.pdf (box C).

As Liu et al (2020)[103] note, oracles introduce risk in a number of ways: their mechanics are opaque and unaccountable; they introduce critical nexuses of trust and dependency into DeFi, and malicious oracles can cause catastrophic harm. The authors find repeated operational failures in the methodological approaches to aggregating data across multiple exchange venues, introducing operational risks and producing poor outputs.

As pointed out by Werner et al (2021),[104] market dislocations at spot exchanges feed into oracles and affect DeFi systems built atop these price feeds. When the thinly-traded stablecoin Dai briefly traded at $1.30 (it is typically pegged to $1) on Coinbase, this unnaturally high premium was fed into the Compound protocol's price feed, leading Compound to automatically decree that a number of accounts were in default and programmatically deleverage and liquidate $88 million worth of collateral.[105] These wrongful liquidations occurred because the protocol designers had assumed that Dai would not trade at a significant premium on referenced markets and, thus, did not have safety checks built in.

c. Excessive leverage: smart contract-based flash loans

Certain idiosyncratic features of DeFi introduce attack vectors that are entirely novel. Among these is the flash loan concept. Proposed in 2020 by DeFi lender Aave, the flash loan is an unsecured loan permitting a borrower to access an unlimited amount of liquidity (up to the size of the loan pool)[106] with a very low interest rate.[107] The catch is that the loan must be paid back within the same transaction that it is taken out. Since DeFi applications give rise to frequent arbitrage opportunities, such short-term loans allow individual parties with limited access to capital to obtain leverage and take advantage of mispricings as long as transactions can be executed atomically (i.e., simultaneously). As transactions on Ethereum can invoke many contracts synchronously, flash loans are a useful tool in inter-contract arbitrage, as described by Wang, et al (2021).[108]

---

[103] Liu, B., Szalachowski, P., and Zhou, J. "A First Look into DeFi Oracles" arxiv.org (11 Dec 2020). https://arxiv.org/pdf/2005.04377.pdf

[104] Werner, et al (2021). https://arxiv.org/pdf/2101.08778.pdf

[105] Khatri, Yogita. "DAI price increase led to a massive $88 million worth of liquidations at DeFi protocol Compound" The Block (Nov. 26, 2020). https://www.theblockcrypto.com/post/85850/dai-compound-dydx-liquidations-defi

[106] The Aave flash loan pool, as of Apr. 12, 2021, offers over $2.5b worth of liquidity. See, https://aavewatch.com/

[107] Aave FAQ, "Flash Loans." Accessed Apr. 13, 2021. https://docs.aave.com/faq/flash-loans

[108] Wang, D., Wu, S., Lin Z., Wu, L., Yuan, X., Zhou, Y., Wang, H., and Ren, K. "Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem" arxiv.org (Mar. 3, 2021). arXiv:2010.12252v2 [cs.CR] 3 Mar 2021 https://arxiv.org/pdf/2010.12252.pdf

Flash loans dramatically reduce the barriers to entry for potential attackers while increasing their leverage, and hence, the financial impact of their attacks on DeFi. Ever since their introduction, flash loans have become increasingly prevalent in DeFi attacks. Cao et al (2021) identified nine separate instances between February and December 2020 in which attackers successfully siphoned a total of $49.58 million (USD value at the time of exploit) from DeFi protocols through flash loan-assisted exploits.[109] The largest of these, the Harvest Attack in October 2020, saw the attackers extract $26 million from Harvest, using the Curve and Uniswap protocols while relying on a flash loan from Uniswap v2. While flash loans could be a helpful tool, they can be misused to dramatically empower would-be attackers by making trial and error costs cheap and granting near-unlimited leverage – provided that transactions can be constructed so that the loan is paid back instantly.

iv. Other governance and regulatory risks

a. Administrative key abuse

Many DeFi protocols retain the discretionary option for administrative teams or other entities to shut them down, upgrade them, pause the contract, and in some cases, drain user funds. There are a few exceptions, like Uniswap, which simply exists as deployed code on Ethereum that users can freely choose to interact with. The Uniswap contracts themselves cannot be paused by the developer team.[110] The vast majority of protocols, however, do retain some form of a control feature, including kill switches. In some cases, critical smart contract decisions are delegated to the community of token holders (although in practice this collapses back to granting decision-making power to a small number of insiders and backers as voting weight is typically proportional to one's share of tokens held). Additionally, since tokens are generally available on the open market (which trades 24/7 on DEXs with no identity verification), an attacker could freely purchase or borrow tokens in order to influence a token holder vote. Thus, many projects for which token holder votes can influence the contract choose to retain de facto control by directly limiting the free float of tokens. As the St Louis Fed notes regarding admin keys, "If the keyholders do not create or store their keys securely, malicious third parties could get their hands on these keys and compromise the smart contract. Alternatively, the core team members themselves may be malicious or corrupted by significant monetary incentives."[111]

A common practice in mitigating admin key risks is granting a consortium of delegates control over critical smart contract decisions by distributing power over key-related decisions into a

[109] Cao, Y., Zou, C. and Cheng, X. Shanghai Wanxiang Blockchain Inc. "Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem" arxiv.org (Feb. 1, 2021). https://arxiv.org/pdf/2102.00626.pdf
[110] Adams, H., Zinsmeister, N. and Robinson, D. "Uniswap v2 Core" White Paper. (Mar. 2020). https://uniswap.org/whitepaper.pdf
[111] Schär (2021), *supra*.

multi-sig setup. Some other controls exist, including enforced timelocks on key-related decisions as is the case with Yearn,[112] or by granting signatories a limited, pre-specified set of powers, as done by Synthetix.[113]

The existence of admin keys in the majority of high-profile, active DeFi projects raises a number of risks. Chiefly, these include key loss, insider theft of deposits, theft through extortion or hacks from outside parties, and regulatory pressure. In many setups, including that of Synthetix, contracts can be unilaterally frozen for a period by insiders as a precautionary 'rapid response' mechanism in the case of a hack or exploit. However, while merely pausing a contract does limited harm, it could adversely affect liquidity.

Ultimately, assets held in contracts mediated by admin keys should be understood as custodial rather than wholly sovereign interactions between users and a protocol. Adding more signatories to a multi-sig key setup simply means that user deposits are held in the custody of a consortium of insiders, rather than by one entity.

Research into the presence of admin keys is sparse because practices are constantly evolving. While major DeFi projects have made efforts to mitigate key man risk and eliminate critical points of centralization with regards to admin keys, independent researchers have nevertheless identified DeFi applications where administrators have unilateral control over user funds.[114] Today, the major DeFi protocols Synthetix, Yearn, Dharma, SushiSwap, Badger, Harvest, and Ren – containing user deposits of $10.58 billion collectively as of Apr. 12, 2021[115] – maintain admin keys enabling a discretionary freeze of user funds.

While the power vested in admin keys varies, in some cases, anonymous individuals retain the right to siphon all liquidity allocated to contracts they administer. Notably, the anonymous admin behind Harvest Finance, which once held over $1 billion in user deposits in its smart contract, can drain user funds encumbered only by a 12-hour timelock.[116] Projects like these, while deployed on public chains, are dubiously decentralized, as they are functionally indistinguishable from centralized asset-taking institutions (albeit not regulated as such).

---

[112] Coopahtroopha, Supra. https://gov.yearn.finance/t/yfi-minting-ownership/155

[113] Synthetix. "Synthetix Foundation Decommissioned" (Jul. 28, 2020). https://blog.synthetix.io/synthetix-foundation-decommissioned/

[114] See, Blec, Chris. "The Trustlessness of DeFi's Top 10 Richest Products" Surviving DeFi (Nov. 23, 2020). https://survivingdefi.substack.com/p/the-trustlessness-of-defis-top-10 See also, Mapperson, Joshua. "How many DeFi projects still have 'God Mode' admin keys? More than you think" Cointelegraph (Sept. 25, 2020). https://cointelegraph.com/news/how-many-defi-projects-still-have-god-mode-admin-keys-more-than-you-think

[115] See https://defipulse.com/ Accessed April 12, 2021.

[116] Blec, Chris. "Hunting Harvest's Admin Key" Surving DeFi (Oct. 23, 2020). https://survivingdefi.substack.com/p/hunting-harvests-admin-key

Some efforts exist to quantify and monitor the risks that users face from the existence of admin keys: the DeFi Watch project, for instance, is a crowdsourced community project that monitors the presence of admin keys in DeFi systems and evaluates their trustlessness.[117] Disclosure of administrative powers by core teams, token holders, and other entities has been poor. For most projects, the scope of powers afforded by admin keys remains opaque, as the developers creating these contracts seek to avoid the perception that they have control over user balances.[118]

b. Governance attacks

As more blockchain-based projects aspire to transform corporate business models by undertaking a decentralized governance model, they introduce new risks. In practice, development teams have been sluggish to delegate genuine decision-making power over development decisions and system parameters for keys, which has meant that few governance attacks have been observed thus far. However, should regulators see through the veil of decentralization[119] erected to obfuscate the true nexuses of control in DeFi protocols, they would see that certain development teams have sought to distribute governance power to holders of "governance tokens." These governance tokens endow their holders with and often a claim – albeit, frequently a diffuse one – on cash flows or fees generated by these systems, as voting power over system parameters. Typically, these have been managed, limited experiences, whereby governance token holders could not vote to, for instance, fire the core development team or redirect funding from the core corporate entity or nonprofit managing the system.

As token holders assert themselves, however, and gain the capacity to be more activist investors, new classes of governance attacks emerge. Activists could elect to exploit DeFi systems to benefit token holders (through some established extractive mechanism) at the expense of the users of these systems.[120] One such attack, according to Gudgeon, et al (2020),[121] permitted a governance attacker who gained control of the MakerDAO system to siphon off $500 million worth of capital from the system (containing at the time $702 million worth of collateral). As governance tokens become more available for short-term liquidity – in particular through flash loans (discussed above), activists can more easily exploit governance token votes to manipulate system parameters. The usage of flash loans to influence the outcome of governance votes has been empirically noted[122] in the MakerDAO system.

---

[117] See, https://defiwatch.net/

[118] Walch, Angela. "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems" SSRN (Feb. 13, 2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244

[119] *Id.*

[120] See, LongForWisdom."[Urgent] Flash Loans and securing the Maker Protocol" makerdao.com (Oc. 2020). https://forum.makerdao.com/t/urgent-flash-loans-and-securing-the-maker-protocol/4901

[121] Gudgeon, L. Perez, D., Harz, D., Livshits, B., and Gervais, A. "The Decentralized Financial Crisis" arXiv.org (Feb. 19, 2020). https://arxiv.org/abs/2002.08099

[122] LongForWisdom (2020).

As noted with the STEEM/Hive case study (mentioned above in the subsection on Validator Cartels), tokens held by exchanges on behalf of users have been employed to influence governance outcomes, in some cases against the wishes of these users. Large caches of governance-laden tokens sitting at exchanges could influence them to accept bribes in order to vote favorably on specific proposals or simply could be borrowed on an extremely short-term basis (likely not impairing the exchange's liquidity requirements) to swing a governance vote. For instance, exchanges would naturally look to monetize user tokens held on deposit via flash loans because the flash loans do not impair their ability to process withdrawals (because the term of flash loans is literally zero). Meanwhile, the borrower only needs to hold tokens for the duration of an on-chain vote in order to influence the outcome.

c. Tainted liquidity

At its core, DeFi envisions novel ways to undertake financial transactions. The cryptographic nature of digital assets permits increasingly sophisticated and intricate schemes for managing custody and transactional workflows. Bitcoin, for instance, offers a native multi-sig functionality, whereby transactions can specify advanced conditions required for an output to be spent. As of the time of writing, there exists a lower bound of 900,000 BTC (worth $56 billion at the time of writing)[123] held in known multi-sig setups.[124]

Thus, a novel class has emerged of custodians that maintain keys as a service, allowing individuals and entities engaging in self-custody to take advantage of the sovereign nature of holding one's keys while maintaining the possibility of recourse in the case of key loss. A common collaborative custody model involves a client holding a key in a "hot wallet," a third-party custodian holding one key, and a third key held for recovery, with two keys required for a valid spend.

Engaging in collaborative blockchain transactions, however, can cause custodians to incur liability from regulators such as the Office of Foreign Asset Control (OFAC). Indeed, BitGo, which provides key management as a service in multi-sig transactions, was sanctioned by OFAC for providing such services to clients in OFAC-sanctioned Crimea, Cuba, Iran, Sudan, and Syria.[125] Bitcoin payment processor BitPay also settled similar charges with OFAC.[126]

[123] Figures current as of Apr. 13, 2021
[124] See, https://txstats.com/dashboard/db/p2sh-repartition-by-type?orgId=1 Accessed April 13, 2021.
[125] https://home.treasury.gov/system/files/126/20201230_bitgo.pdf
[126] https://www.coindesk.com/bitpay-to-pay-500k-to-settle-ofac-sanction-violation-charges

Additionally, the Financial Action Task Force (FATF) recently clarified in their recently revised draft guidance on virtual assets[127] that parties administering keys in a multi-sig setup risk being considered virtual asset service providers (VASPs), which would subject these parties to surveillance and disclosure obligations, as well as to Travel Rule compliance requirements.[128] According to Coin Center, the FATF draft guidance breaks with policy precedent from the Financial Crimes Enforcement Network (FinCEN), which considers "only persons with 'independent control' over customer funds are treated as regulated money transmitters."[129] The revised FATF draft guidance would dramatically increase the scope of covered parties.[130]

DeFi in its current form is largely incompatible with such regulations. Since most decentralized contracts do not require any user identification beyond a valid blockchain address, there is virtually no emphasis on centralized compliance. Products facilitating on-chain swaps, like Uniswap, are simply blockchain contracts that permit users to collaboratively pool funds and make trades with no central intermediary.[131] [132] The nature of these "peer-to-pool" systems is such that these contracts cannot meaningfully exclude any entity looking to participate in the pooling, which is open and freely participatory by definition.

Uniswap, in particular, relies on "liquidity providers" that contribute assets to a pool in exchange for fees. These are not designated entities; anyone can be a liquidity provider if they contribute assets to the pool. At the time of writing, Uniswap v2 boasted 84,000 active liquidity providers with 5,400 liquidity providers active in the most popular pair, UNI-WETH.[133] If some tainted liquidity, for instance emanating from an OFAC-sanctioned party or an illicit source, were to enter a Uniswap pool, regular users would effectively be undertaking a financial relationship with these prohibited parties. As currently deployed, the smart contract has no means to whitelist users or permission them *a priori*. The very nature of decentralized finance on public blockchains like Ethereum is to facilitate permissionless exchange, but this open access is generally incompatible with anti-money laundering/combating the financiang of terrorism (AML/CFT) regulations as currently implemented in the U.S.

---

[127] FATF "Draft updated Guidance for a risk-based approach to virtual assets and VASPs" (March 2021). https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf

[128] See, Van Valkenburgh, Peter. "A quick analysis of FATF's 2021 draft cryptocurrency guidance" Coin Center (Mar. 22, 2021). https://www.coincenter.org/a-quick-analysis-of-fatfs-2021-draft-cryptocurrency-guidance/

[129] *Id*.

[130] Specifically, the recent FATF draft guidance notes in para. 54 that "[t]his control [over client assets] does not have to be unilateral and multi-signature processes are not exempt" when evaluating whether an entity should be considered a VASP."

[131] For an introduction to Uniswap, see, Angeris, G., Kao, H., Chiang, R., Noyes, C., and Chitra, T. "An analysis of Uniswap markets" arxiv.org (Nov. 2019). https://arxiv.org/pdf/1911.03380.pdf

[132] Note: Aave's new permissioned pool is an exception.

[133] Source: https://explore.duneanalytics.com/dashboard/uniswap-community as of April 13, 2021.

d. **Pseudo-equities - regulatory uncertainty**

Transactions that involve lending, investment trading, and derivative exposure are regulated in traditional financial markets through the registration, licensing and examination of intermediaries that broker, custody, clear or otherwise facilitate such transactions. In DeFi, intermediaries are largely excluded in favor of transparent code, presenting regulators and policymakers with complicated decisions as to how to assess transactions (often bilateral) for which no clearly identified party may be regulated. These important issues regarding the regulatory uncertainty of the underlying commercial transactions that are conducted through DeFi protocols are beyond the scope of this paper. This sub-section, however, examines more specifically so-called 'pseudo-equities' and their inherent regulatory risks.

Despite considerable regulatory risks of issuing pseudo-equity tokens with little regard for the requirements of securities law, many DeFi protocols are administered by U.S.-based firms or nonprofits.[134] In many cases, these entities finance themselves through the issuance of a token that represents a claim on some cash flows produced by the system. These tokens have proven to be a meaningful financing vehicle for developing DeFi protocols. As the time of writing, the aggregate market capitalization of tokens in the "decentralized finance" space is $85 billion, with Uniswap, Synthetix, and Compound (collectively having taken in $12.29 billion[135] in allocated collateral) being the largest pseudo-equity tokens. Many of these DeFi tokens endow token holders with some rudimentary governance rights as well as either implicit or direct claims on cash flows generated through DeFi protocols. None of these pseudo-equity tokens backstopping DeFi are registered as securities, circulating instead on decentralized financial infrastructure like Uniswap (and in some cases, on centralized crypto exchanges). If securities regulators deemed such pseudo-equity tokens to be unregistered securities and pursued not only their issuers and promoters but also the venues upon which they trade, the financing and governance model of these DeFi projects would be significantly impaired. Additionally, numerous DeFi protocols subsidize their liquidity by issuing new units of pseudo-equity to end users. If these tokens were to be delisted and their liquidity and value suffered losses, the utility of these subsidized protocols would decline. These token incentives built into DeFi protocols are the equivalent of Uber compensating drivers for each mile driven with incremental units of Uber equity. As an example, the compensation for supplying the stablecoin USDC to the money-market protocol Compound is 6.71% annualized at the time of writing, supplemented by a 2.15% annualized payout in COMP terms to suppliers of USDC. The combination of the two is described as the 'net rate' for USDC by Compound.[136] If these incentives were to expire or be withdrawn, interest

[134] Precedent exists for SEC enforcement actions regarding U.S.-based entities administering smart contracts, including the case of EtherDelta, in which the founder administered frontend smart contracts governing token trading on the Ethereum network, is best known. The SEC considered EtherDelta an unregistered national securities exchange. See, https://www.sec.gov/news/press-release/2018-258
[135] Figures taken from https://defipulse.com/. Current as of April 12, 2021.
[136] https://compound.finance/markets/USDC

rates would look significantly less attractive, reducing the incentive for liquidity providers to put their capital at risk.

Virtually all DeFi protocols require oversight, bug remediation, technical and economic audits, governance stewardship, and leadership and direction from these administrative entities. Even if there are no corporations or firms officially underwriting these decentralized protocols, virtually all of these protocols have an entity, whether codified or not, effectively managing the protocol. The elimination of the pseudo-equity token as a viable financing mechanism would significantly impair the industry's ability to operate. It is possible, however, that corporations could create the majority of decentralized finance contracts and monetize them without the use of a token by directly charging rents for usage of the DeFi contract, or that anonymous developers could deploy these protocols to the blockchain.

v. Challenges associated with scalability

Scalability – the general process whereby public blockchains grow to handle an economically meaningful volume of activity and more transactional data without compromising their assurances – is held as one of the chief difficulties facing blockchains today. Adding more data to the final ledger trades off against the computational difficulty of operating a full node and staying current on the ledger. While no silver bullet solution to scalability of blockchain exists, since the basic security model of blockchains requires that all participants store a full copy of the state, various improvements have been proposed.[137]

Approaches such as Bitcoin's Lightning Network envision a network of payment channels with only periodic final settlement to the Bitcoin layer itself.[138] Sidechains immobilize bitcoins (or other native units) and create a subledger whereby claims on those Bitcoins can circulate frictionlessly, effectively creating a new transactional space.[139] [140] Sharding splits the state of the blockchain into parts, with nodes finding consensus on a subset of the final state, periodically

[137] For a more complete overview of scalability solutions, see Kim S., Kwon, Y., Cho, S. "A Survey of Scalability Solutions on Blockchain" 2018 International Conference on Information and Communication Technology Convergence (ICTC) (Oct. 17-19, 2018). https://ieeexplore.ieee.org/abstract/document/8539529

[138] Poon, Joseph and Dryja, Thaddeus. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" Draft Version 0.5.9.2 (Jan . 14, 2016. http://lightning.network/lightning-network-paper.pdf

[139] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timon, J., and Wuille, P. "Enabling Blockchain Innovations with Pegged Sidechains" (Oct. 22, 2014) (commit 5620e43). http://kevinriggen.com/files/sidechains.pdf

[140] A "sidechain" is a subledger where transactions occur off-ledger, and are periodically settled to the base layer itself (blockstream paper on sidechains).
"Roll-ups" similarly involve performing computation off-ledger, then periodically posting the results of that computation to the blockchain itself.

reconciling with each other.[141] [142] More creatively, rollups (primarily envisioned for computation-heavy blockchains like Ethereum) bundle transactions, moving computation on-chain, but retaining final transactional data on chain. The validity of these transactions is assured through zero-knowledge proofs or mechanisms known as fraud proofs.[143]

The commonality around all these approaches is transactional parsimony, or the reduction of a transaction into as few final bytes as possible, since the costs associated with storing and processing transactional data is the chief externality of blockchain transactions. Unless radically new models for public blockchains are developed, the problem of scalability will be an inherent constraint, as it follows naturally from the requirement that nodes must ingest and verify the global state in order to become full participants on the ledger. Additionally, these approaches all generally aim to defer final settlement by distinguishing a payment or financial message and the settlement of that message or bundle of transactions. This deferred settlement mechanism will be familiar to anyone with knowledge of established payment systems, but public blockchains have only just begun to explore their implications.

As mentioned, public blockchains in their current form are effectively deterministic, single state environments[144] in which each peer must process each and every transaction in order to stay in sync in a trustless manner with the blockchain's current state. Both Bitcoin and Ethereum have committed to operational limits on the most data throughput that either system can handle, with Ethereum adopting a looser constraint. These limits roughly correlate with the number of transactions that consumer hardware can meaningfully process without falling behind. In order to prioritize transactions, both systems employ fees. Naturally, some classes of users are more willing to bear fees than others, with fee sensitivity generally being a function of the perceived importance of a transaction. The consequence of this approach means that, in their current format, heterogeneous demand requires that some applications are naturally priced out at any given time. Applications of Ethereum are varied, running the gamut from using stablecoins for remittances, to operating decentralized organizations, to minting non-fungible tokens that represent unique pieces of artwork, to financial use cases like obtaining programmatic leverage. Since all of these applications are competing for the same finite pool of blockspace, a burst of adoption for one use-case can degrade the experience of using another (due to the effect of fee

---

[141] Schaffner, Tobias. "Scaling Public Blockchains: a comprehensive analysis of optimistic and zero-knowledge rollups" University of Basel (Jan. 14, 2021). https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Schaer_DLTFintech/Lehre/Tobias_Schaffner_Masterthesis.pdf

[142] "Sharding" is a process whereby the ledger state is partitioned and transfers occur locally within the shard, and are periodically reconciled with the global state.
Each model involves effectively partitioning state in order to gain transactional efficiency and subsequently reconciling it with the global ledger

[143] Schaffner, *supra*.

[144] 'Single-state' means that all participants share the same ledger. 'Determinism' is the property whereby the same inputs should always lead to the same outputs.

hikes on the market for blockspace). High fees have the effect of pricing out smaller transacting parties, who might deem an operation uneconomical if fees hit a certain threshold.

Due to relatively inelastic blockspace combined with volatile demand for blockchain resources, fees are highly volatile. For instance, on February 23, 2021, mean per-transaction Ethereum fees reached $38 while mean Bitcoin fees reached the equivalent of $25.[145] For comparison, in 2019, Bitcoin and Ethereum per-transaction fees averaged the equivalent of only $1.24 and $0.13,[146] respectively.[147] In addition to the general drag that fees introduce on transactional usage, blockchain congestion can facilitate specific attacks against DeFi protocols, which sometimes need to execute transactions within a specific period. On March 12, 2020, for instance, the MakerDAO system became insolvent as on-chain liquidations of ether were processed at the price of $0 (instead of the market rate of $120) per coin resulting from lagging liquidation engines, which could not get transactions processed in time due to high fees.[148] This caused a loss of $8 million to holders of debt positions in the MakerDAO system and left the Dai stablecoin undercollateralized by $4.5 million.

Additionally, as fees rise on blockchains, they price out certain classes of activity, especially more computationally expensive actions (particularly for blockchains like Ethereum where the cost to transact is a function of computational demand). This systematically prices out users with smaller balances and has the net effect of trapping funds held in accounts (or UTXOs, in the case of Bitcoin), stranding those assets. As fees rise on the base layer, retail users can no longer economically engage in DeFi operating on the base layer, affecting liquidity in decentralized exchanges.[149] In Bitcoin, a negative feedback loop between transactional usage and fees was evident in 2017-18, indicating that fees not only adversely affect users' affinity to transact, but they do so in an inherently unstable way, without finding equilibrium.[150]

---

[145] Coin Metrics. Accessed Apr. 12, 2021. https://network-charts.coinmetrics.io/

[146] See, https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[147] And for further comparison - wire transfer fees generally range from $15-$30. Credit card processing fees range from 1.43 to 3.5 percent of the transaction amount. For Venmo, zero transaction fees for transfers to linked bank account, debit card or Venmo account, but if Venmo users want to access cash earlier than 1-2 days, then instant transfers from Venmo to linked debit card requires a fee of 25 cents or 1% of the total transfer, whichever number is higher. https://www.mybanktracker.com/news/wire-transfer-fee-comparison-top-10-us-banks , https://www.bankrate.com/finance/credit-cards/merchants-guide-to-credit-card-processing-fees/ , https://www.credit.com/blog/the-app-your-kids-are-using-to-pay-people-back-venmo/

[148] See, Eichholz, Liesl. "What Really Happened to MakerDAO" Glassnode.com (Mar. 17, 2020). https://insights.glassnode.com/what-really-happened-to-makerdao/ See also, Blocknative. "Evidence of Mempool Manipulation on Black Thursday: Hammerbots, Mempool, Compression, and Spontaneous Stuck Transactions. (July 22, 2020). https://www.blocknative.com/blog/mempool-forensics

[149] Carter, Nic. "Public blockchain fee cyclicality and negative feedbakc loops" medium.com (Oct. 5, 2020). https://medium.com/@nic__carter/public-blockchain-fee-cyclicality-and-negative-feedback-loops-1620141a8a87

[150] More descriptive data regarding bitcoin fee dynamics can be found in Lehar, A. and Parlour, C. "Liquidity Demand and BitCoin Transaction Fees" (May 2019) (preliminary and incomplete). https://iwfsas.org/iwfsas2019/wp-content/uploads/2017/02/S4_P2.pdf

DeFi protocols depend critically on seamless interoperability as well as on composability.[151] Gudegon, et al (2020) stress the importance of composability on these systems: "Assets that are created in Maker, for example, can be used as collateral in other protocols such as Compound, dY/dX, or in liquidity pools on Uniswap." Thus, mitigating the impact of base-layer fees by creating subledgers or deferred settlement processes like sidechains, rollups, or sharding does little to solve the problem at its core. Deferring settlement introduces efficiencies by engaging in periodic reconciliation with the base layer itself. However, DeFi as currently envisioned depends on funds being available on the base layer and contracts being able to seamlessly communicate and refer to each other. Thus, standard approaches to scaling appear to compromise the desirable qualities of DeFi and do not represent a panacea to the fee drag. It remains to be seen whether the standard approach to scaling blockchains – effectively mimicking the layered approach that characterizes established payments systems – can be made consistent with the desirable qualities of blockchains that distinguish themselves from these systems. If they cannot, then real estate on the base layer of blockchains with capped throughput will be reserved only for well-capitalized parties, which are able to outbid smaller users.

IV. Conclusion: "No Free Lunch"

The risks described in this chapter do not seek to provide a comprehensive list but to help readers conceptually understand the drivers behind the risks inherent in DeFi. Many of the risks described above stem from the decentralized nature of blockchains. The goal of automating the delivery of financial services and reducing human dependencies also has the congruent effect of reducing oversight and control. Disintermediating traditional intermediaries reduces high fees and entry friction, but also creates new opportunities for new types of intermediaries. These new types of intermediaries require the sufficient economic incentives and, thus, could be potentially more costly and risky than the monopoly rents extracted by today's centralized intermediaries. Ultimately, this new host of intermediaries in a decentralized financial ecosystems could stymie the drive toward the twin goals of democratizing financial services: lowering cost and improving access.

External dependencies on traditional finance, namely banks, is another important source of risk as well as a transmission channel for risk. Although one of the goals of DeFi is to create a new kind of financial system without traditional intermediaries, the irony is that as DeFi struggles to make itself more useful in the real world, its dependency on the established financial system

[151] Composability refers to the assurance that a transaction being proposed which calls multiple distinct contracts will execute, because each implies final settlement. Gudgeon, et al (2020) describe it as "the ability to build a complex, multi component financial system on top of crypto-assets" while Wachter, Jensen and Ross note that it limits the "role for central clearing counterparties in mitigating counterparty risk." https://arxiv.org/ftp/arxiv/papers/2102/2102.04227.pdf

grows. Its reliance on traditional finance is not only a source of risk but can potentially serve as a transmission channel for risk between traditional financial and DeFi systems. DeFi leveraging stablecoins' backing by fiat or other financial liabilities is an excellent example of this type of risk. Another dependency is that the crypto industry still needs to bank with commercial banks in order to conduct the cash legs of their transactions.

DeFi is developing in a direction different than originally intended and, thus, it is coming full circle. The tools exist to wall off DeFi from the financial system, such as running everything on native tokens DAI or ETH for instance. However, the opposite is occurring. Relying on commercial banks for stablecoins (etc) is convenient and serves business needs.

Wholly new risks are introduced by DeFi stemming from the reliance on open protocols and the fact that the underlying infrastructure is un-owned. Removing the back office and human oversight results in many efficiencies, but they also introduce risks. Thus, it is up to the end user or contract administrator to monitor the risk of the protocols themselves, and many would not want the burden. These risks are amplified when financial primitives collide with automated, hard-to-intervene contracts. Here is where all the chaos in DeFi is really from - systems that are built to be scalable and automated but that are underspecified or not understood by their creators. In sum, blockchain technologies bring many benefits. But the tools or processes used to disintermediate or gain efficiency also have costs in recourse, reversibility, risk management, etc. – the 'paradox' of DeFi.

In spite of this 'paradox,' DeFi is achieving something truly novel: it is facilitating the business model experimentation and evolution in a very short time frame. While our traditional financial system has evolved over centuries to reach our current institutional arrangements (i.e., banks, financial markets, market participants, different types of regulation – each in response to past crises and mis-steps), DeFi is allowing for significantly more rapid institutional innovation and trial and error experimentation. There is a lot of error at the moment (lots of speculative bubbles, fraud, governance issues, etc.), but those innovations that persist over several years in such a fast-moving environment could be much more robust. As DeFi becomes more economically relevant, financial stability risks in DeFi could come not only from the links with the traditional financial sector but also from the risks within the DeFi sector itself. More research is needed to study how shocks in the DeFi sector can impact the greater financial system and the real economy. There's a greater need than ever to research this understudied but increasingly important area to help provide a better understanding of the evolution of financial services and the risks inherent in DeFi for industry, regulators and policymakers.