Systemic Risk in the Digital Assets Ecosystem

Michael D. Norman, Ph.D.[1,2], Yiannis G. Karavas[1], Michael D'Acampora[1], and Sanith Wijesinghe, Ph.D.[1]

[1]MITRE
[2]Consensys

August 2024

The purpose of this paper is to generate systemic risk-reducing recommendations for future research directions in the digital assets ecosystem through the lens of a complexity science-based framework. Here we highlight potential systemic risk vulnerabilities associated with four digital asset market features; a) decentralized exchanges, b) decentralized money markets and lending, c) decentralized autonomous organizations and d) decentralized liquidity. For each ecosystem feature we provide a detailed description of its functionality, underlying transaction flows and potential scenarios that could lead to risk propagation. In closing we provide a complex systems-based framework to characterize the vulnerabilities of each ecosystem feature and hypothesize approaches to address risks from a first principles-based perspective.

1 Introduction

The crypto market has experienced rapid growth and evolution, raising concerns about systemic risks and the need for effective regulatory frameworks. Examples abound, from the collapse of the endogenously-backed Terra Luna (UST) stablecoin[1], to FTX's low-float, high fully-diluted value reserves ploy imploding during a liquidity crunch[1], to more recently the on-chain depeg[3]

[1]In a nutshell, FTX was securing customer deposits by marking-to-market a few coins that they held the vast majority of, and were constantly using customer funds to buy them back on the open market to support their price, and therefore appear solvent on paper[2]

of USDC to the US dollar as a result of the run on, and subsequent collapse of, Silicon Valley Bank[4] – demonstrating that systemic risk can flow from the traditional financial system to the digital asset ecosystem. These examples expose some of the type of vulnerabilities that can lead to greater contagion.

This paper presents a series of examples of digital asset ecosystem components and the potential risks they each may engender, especially when monitored within a traditional entity-based financial regulation paradigm. We focused on systemic risk in the decentralized web (web3) as a whole, with a specific, but not exclusive, focus on decentralized finance (DeFi). We will begin our exploration with the most prominent use case for the ecosystem: the trading of digital assets. We will go 'under the hood' to understand how a set of diverse agents is able to, in a completely decentralized manner, create the emergent functionality which allows the trading of assets without any intermediary entities.

Next, we explore the second most prominent use case in DeFi: money markets and lending. These ecosystem components provide decentralized and permissionless lending at interest rates that were highly enticing during the prolonged near-zero rate environment in the US banking system, and on the other side, enabled borrowing in the same manner. As our third conceptual example of the disruptive innovation provided by the digital assets ecosystem, we explore the new types of trustless and open human organizations that have emerged, commonly referred to as decentralized autonomous organizations (DAOs). Our fourth example focuses on one of the more salient systemic risk vectors across all types of markets, but with a specific focus on its presence in the digital assets space: liquidity.

By synthesizing these examples, we provide insights into the challenges associated with applying traditional financial regulation at an entity level to this domain. Finally, we zoom out and propose a more generalized perspective on this ecosystem by viewing it through the lens of complexity science[5]. Although only the first step in this direction, we believe with further research and development this point of view will enable a more effective means of understanding and mitigating systemic risk. We close with a set of recommendations and next steps for future research.

2 Risk Vulnerabilities in Decentralized Exchanges and Liquidity Pools

Decentralized exchanges (DEXs) facilitate crypto asset trading in the web3 ecosystem without a centralized order book, instead utilizing liquidity pools where participants, known as liquidity providers, supply asset pairs to enable trades and earn transaction fees. These liquidity pools are governed by Automated Market Maker (AMM) protocols, which automate the exchange process without intermediaries. Trading fees are split between the protocol's treasury and liquidity providers, proportional to their contribution to the pool. A significant risk for liquidity providers is impermanent loss, which occurs when the relative price of tokens changes, affecting the value of their deposited assets.

Uniswap, a prominent DEX on the Ethereum blockchain, has undergone three major updates to enhance its functionality. Uniswap V1 introduced ETH-ERC20 liquidity pools and a constant product formula for AMM, while V2 allowed for any ERC-20 token pairs and improved price

oracles. Uniswap V3 introduced concentrated liquidity, enabling providers to allocate capital within specific price ranges, though this complexity has shifted the user base towards more professional market makers. Other notable DEXs include SushiSwap, PancakeSwap, GMX, dYdX, and DOPEX, each contributing unique features to the decentralized trading landscape (see Appendix A for further details).

2.1 Potential Risk Mechanisms

2.1.1 Low Liquidity Exchanges

Low liquidity in a particular market makes it more expensive to transact in due to wider bid-ask spreads and is more vulnerable to price shocks, which can reduce market participation over time. More importantly, it is easier for bad actors to manipulate prices since it requires less capital to cause significant price swings. If multiple protocols rely on the manipulated market for an external price feed, it could create a cascading effect across multiple venues and create a system risk across the ecosystem.

There are exchanges and tokens with low liquidity that can cause such systemic risk as described above; one such example was the MANGO Markets exploit[6]. Such manipulations due to low liquidity may not only prove harmful as standalone events but can also be used to trigger second order effects such as oracle (price feed) manipulations. Combining such tactics with leverage can create a lot of instability which can lead to cascading failures. Doing so using leveraged products on GMX or dydx could exacerbate such exploitative events.

2.1.2 Liquidity Fragmentation

The permissionless nature of the digital assets ecosystem enables the emergence of many markets for a single asset. This stands in stark contrast to centrally-planned markets, such as CFTC-regulated commodities futures markets, which provide solitary deep liquidity sources for participants to gain market exposure via top-down regulation. Fragmented liquidity as a risk vector will be further explored in the proceeding pages.

2.1.3 Decentralized Finance and Traditional Finance Interconnectivity

Connections points between the worlds of DeFi and traditional finance (TradFi) continue to increase and will likely result in greater overall systemic risk transmission from one ecosystem to the other[7].

The most prominent foci of current TradFi-DeFi connectivity is the introduction of ETP/ETF-based wrappers for spot BTC and ETH. At the time of writing, a plethora of BTC ETFs have been actively traded in TradFi markets. The market's appetite for Blackrock's IBIT was described shortly after its launch by Blackrock CEO, Larry Fink:

> *"IBIT is the fastest-growing ETF in the history of ETFs. Nothing is gaining assets as fast as IBIT in the history of ETFs"*[8]

Any lingering doubts as to the direction of travel of TradFi-DeFi interconnectivity should be put to rest by this fact.

Further intertwining the old world with the new, ETP/ETF-wrapped ETH will launch shortly; SEC approval was granted on 23 May 2024[9]. Although the magnitude of the impact of ETH ETFs is currently left to speculation, there is no question that long term capital inflows will occur.

A future where large sets of individual retirement accounts, massive pension funds, and other large entities have significant exposure to digital asset volatility is now highly probable. For this reason, potential future crypto market crashes will undoubtedly have spillover effects on TradFi.

As institutional investors and traditional finance firms enter the DeFi space, they may introduce their own sources of systemic risk. Traditional financial institutions often have complex balance sheets and large counterparty exposures, which can create vulnerabilities if not managed properly. Conversely, if a significant issue arises in the DeFi sector, it can impact traditional financial institutions, especially those with significant exposure to DeFi assets or platforms. This two-way risk transmission can amplify the consequences of disruptions in either system, and their increasing interconnectivity can lead to contagion effects.

Interestingly, the DeFi space is characterized by its real-time, trustless, open, and transparent nature, while traditional finance often operates with a degree of opacity, with trust-based disclosures coming out at a much slower cadence. In either case, market participants need to have a complete understanding of the risks associated with their investments, particularly as the complexity of DeFi products and their connection to traditional finance increases. When there are no central actors to hold accountable for disclosure of technical or financial risk of the parts of an ecosystem then the need emerges for an entity or set of entities to produce these disclosures for the investing public's consumption. Further, it would be useful for an entity or set of entities to provide system-level risk disclosures/analysis, perhaps in the same vein as banking system stress tests. The transparency and decentralized nature of the DeFi ecosystem relative to TradFi requires a complex systems-based technical approach to risk disclosure; one that is focused on emergence and cognizant of the underlying social dynamics upon which the system's technical foundations rest.

Recent events such as the Terra/Luna ecosystem collapse in DeFi and the collapse of Silvergate Bank, Silicon Valley Bank and abrupt closure of Signature Bank have demonstrated the possibility for systemic risk to make its way from either system into the other[10]. Due to limited interconnectivity between these ecosystems at that point in time, however, there was limited spillover.

Recommendation for Future Research

Developing increased understanding of new financial phenomena such as Automated Market Makers, their construction, and alternatives; impermanent loss in liquidity providing positions; bad debt accumulation in loan liquidation events; algorithmic stablecoins and mint/burn mechanisms; the implications/consequences of such phenomena in various scenarios from steady state operation of their surrounding ecosystem to extremely stressed operation (including the occurrence of long-tail events).

3 Risk Vulnerabilities in Decentralized Money Markets and Lending

Decentralized money markets facilitate lending and borrowing of assets without intermediaries, relying on smart contracts on blockchain platforms. Unlike traditional money markets, they offer open accessibility without eligibility requirements, though loans typically need to be over-collateralized due to the volatility of digital assets. Interest rates in decentralized money markets are driven by supply and demand algorithms or governed by Decentralized Autonomous Organizations (DAOs), providing real-time market insights and potentially more competitive rates.

Borrowers must fulfill collateral obligations, and if the collateral's market value falls below a certain Loan-to-Value (LTV) threshold, it is liquidated by the protocol. Different protocols use various algorithms to manage risk and enforce liquidation rules. Compound Finance, a prominent decentralized protocol on the Ethereum blockchain, manages pooled liquidity and interest rates through smart contracts, enabling users to lend and borrow digital assets without intermediaries. As of April 2023, Compound manages approximately $750 million in open loans backed by $2.4 billion in collateral.

Compound's infrastructure consists of smart contracts that create money markets for each supported asset, pooling liquidity from various sources. Interest rates are algorithmically determined based on the utilization ratio, with rates rising as utilization increases to incentivize more asset supply. Users receive cTokens representing their supplied assets and accrued interest, which can be redeemed at the prevailing exchange rate. Borrowers must supply collateral and maintain a minimum level of collateralization to avoid liquidation.

Compound integrates easily into other DeFi applications, allowing developers to build new products and services on its infrastructure. However, it is subject to risks such as smart contract vulnerabilities and market volatility, which are mitigated through regular audits and security best practices. Other notable decentralized money market protocols include Aave, Alchemix, Liquity, Venus, and MakerDAO (see Appendix B for further details).

3.1 Potential Risk Mechanisms

3.1.1 Lending Protocol Debt Accumulation

Lending protocols in decentralized finance can accumulate enough bad debt from faulty liquidation events to create systemic risk if risk is managed improperly[11]. While the probability of such a scenario may be low, its impact could be significant due to the interconnected nature of DeFi protocols.

If the protocol holds a disproportionate amount of a collateral asset and it rapidly loses value, it may be unable to liquidate the collateral fast enough to cover the corresponding loan amounts, resulting in losses. In addition to market-based stressors, a protocol could experience withdrawals from its depositor base to exacerbate the crisis. Robust liquidation mechanisms are paramount, because unlike traditional banking, lending protocols do not yet have a mechanism to recall debt.

If liquidation mechanisms are faulty, slow, or inefficient, they may not be able to liquidate collateral effectively in a panic. The losses from a faulty liquidation would fall squarely on

depositors, since it is their funds that the protocol is lending. An event where depositors lose could then cause a run on the protocol's entire deposit base, fearing other collateral could be unnecessarily lost due to faulty liquidation processes. Considering the interconnectivity in DeFi, cascading failures could result across the ecosystem.

During periods of high network congestion or elevated transaction fees, liquidators may be programmatically deterred from participating in liquidation events due to gas prices (network transaction fees which scale with congestion) needed to execute the liquidation having a higher cost than the liquidation take itself. This could lead to slower liquidations as agents wait until execution becomes profitable and a higher likelihood of bad debt accumulation. Accumulation of bad debt in one lending protocol can have spillover effects, leading to liquidity crunches, price distortions, and further liquidation events in other protocols, posing systemic risk.

3.1.2 Cyber and Economic Vulnerabilities

Smart contract bugs that could drain lending pools in DeFi lending protocols pose a systemic risk to the DeFi ecosystem for several reasons. As the DeFi space is highly interconnected, an exploit in one protocol can have far-reaching consequences, potentially leading to a cascading failure that affects multiple platforms and users. Note, that when discussing the term "smart contract bug" in this section, it is a reference to cyber-related exploits that utilize poorly written code, configuration or infrastructural zero-days (e.g., The DAO Hack[12]).

DeFi protocols often rely on each other for liquidity, price data, and other services. If a lending pool in one protocol is drained due to a smart contract bug, it can create a domino effect that reverberates throughout the ecosystem. Other protocols that depend on the affected platform may face liquidity shortages or inaccurate price data, leading to further liquidation events, price distortions, and potential losses. Many DeFi platforms use lending pools as sources of liquidity for various financial products, such as stablecoins, decentralized exchanges, or derivatives. If a smart contract bug drains a lending pool, it can disrupt the functioning of these interconnected products, potentially causing a cascading failure that affects the broader ecosystem.

A significant smart contract bug in a lending protocol can also have psychological implications on the market and can lead to a consequent loss of confidence in the affected protocol and the broader DeFi ecosystem. As users become more cautious, they may withdraw their funds from other protocols, causing a liquidity crunch and exacerbating the impact of the original exploit. Further panic selling may even be triggered as well as rapid deleveraging as users scramble to withdraw their funds from the affected protocol and other platforms. This can lead to increased price volatility, reduced liquidity, and a vicious cycle of forced liquidations that can impact the broader DeFi market. This torrent of forced liquidations can lead to aforementioned bad debt in lending protocols if they are performed inefficiently due to undue market strain.

A high-profile exploit resulting from a smart contract bug, such as the infamous DAO hack in 2016, can damage the reputation of the DeFi space as a whole, leading to increased regulatory scrutiny and reduced institutional participation. This can slow down the growth and adoption of DeFi, potentially limiting its ability to compete with traditional financial services and stifling innovation in the sector.

Confining attempts to mitigate risk such as that described above to the contemplative state, merely theorizing about possible causes and their cascading effects can only be effective up to a

very limited degree. In fact, often attacking such problems from a purely theoretical perspective will undoubtedly result in a false sense of security from the belief that all corner cases and downstream effects have been accounted for due to an exhaustive contemplative effort. As with all complex systems, however, analysis likely, if not definitely, requires the use of some sort of modeling such as agent-based modeling.

Most uniquely, DeFi offers less-scrupulous characters a multidimensional economic attack surface via the clever combination of a long-tail of poorly designed and/or low-TVL[2] protocols which emerge in a permissionless environment. The most significant example of recent memory is the Mango Markets economic "exploit". "Exploit" is in quotes because it was not a code exploit in any technical sense, but rather an emergent economic vulnerability that was identified and utilized. The vulnerability is emergent because each individual component of the ecosystem that Avi Eisenburg leveraged to accomplish the capital exfiltration from the protocol was used and operated as their respective designers intended. There was no cyber/exploit aspect whatsoever. The lack of an appropriate lexicon to accurately and succinctly describe the behavior observed here is further indication of the need to aggressively invest public interest-focused cryptoeconomic research, especially from a complexity science perspective.

Recommendation for Future Research

Research, evidence gathering, and an industry-wide coalition are needed to drive a coevolutionary-aware regulatory approach which embraces whitehat ethics, i.e., economic exploits are not to be raised up to legal authorities as long as a predetermined large percentage, e.g., 90%, of exfiltrated value is returned to users, and the method of the economic exploit is documented in a way that allows not just the exploited protocol, but all systems of a similar nature to adapt and bolster their resilience against future actions of this type. The Security Alliance's (SEAL) Whitehat Safe Harbor Agreement[a] is an excellent first step in this direction. If economic vulnerability failures are not often and small, then they will be infrequent and devastating. The web3 ecosystem does not support involuntary asset recovery, thus putting in place a means of legitimately rewarding those who discover economic vulnerabilities, without fear of reprisal, is important long-term for both users and developers.

[a] https://github.com/security-alliance/safe-harbor

"On October 11, 2022, Eisenberg made three massive MNGO perpetual futures trades between himself, pumping the price over 1000% and then using his newly created collateral to trick the protocol into allowing him to "borrow" $110 million in various cryptocurrencies." [13]

There is one important environmental condition that, if not present, would have prevented Eisenburg's economic exfiltration scheme from working: thin liquidity in a perpetual futures market.

[2] Total Value Locked (TVL) is the sum of capital (usually expressed in USD terms) that lives within a smart contract. Commonly used to rank protocols in order of importance. However, even this metric has been gamed and so should not be considered without context. A Solana developer launched a set of interconnected DeFi protocols which tricked normal TVL observations to report multiples of the actual underlying capital.

3.1.3 Leverage

Rehypothecation in DeFi lending defines a strategy where users accumulate higher levels of leverage by recursively using borrowed funds as collateral for further borrowing. As leverage increases, so too does the potential for significant gains or losses, leading to heightened volatility and instability in the ecosystem. Highly leveraged positions have a smaller margin for error, and liquidations can occur with smaller movements in price. As more users engage in rehypothecation strategies, it can trigger tail risk. If risk is not properly managed and lending is not properly collateralized, such risk can lead to spillover to interconnected platforms and ultimately result in a contagion event.

In case of a sharp decline in collateral value, users with leveraged positions may rush to sell their assets to reduce their exposure or meet margin calls. This can lead to panic selling, further depressing the value of the collateral assets and exacerbating the initial problem. Rapid deleveraging can also increase price volatility and reduce liquidity in the DeFi ecosystem, creating a vicious cycle that contributes to systemic risk. Again, such complex systems often require modeling efforts in order to identify such risks as those highlighted above. A purely contemplative/theoretical approach often leaves gaps in risk identification and may even serve to exacerbate those unidentified risks due to over-confidence that all risks have been properly identified already.

It is worth noting also, that undercollateralized lending is still a largely unexplored space within DeFi, and a system such as the fractional reserve system in traditional banking has yet to make a widespread appearance. An improper implementation of such a system in the world of DeFi could lead to even faster and more severe bank runs than those experienced by Silicon Valley Bank recently. Research into implementing such a system in DeFi may be a worthwhile endeavor.

4 Risk Vulnerabilities in Decentralized Autonomous Organizations (DAOs)

Decentralized Autonomous Organizations (DAOs) are community-led entities governed by smart contracts, with no central authority. They manage treasury, product development, and personnel decisions through community voting, where voting power is proportional to governance token holdings. DAOs ensure transparency and accountability, as all decisions and transactions are publicly auditable. Members can create proposals to guide the DAO's trajectory, though requirements for proposal submission vary across DAOs. Revenue for DAOs is typically generated from protocol fees, token sales, partnerships, and staking rewards. Beyond protocol management, DAOs can handle investments, grants, services, social networks, and more, with tools like DAO creation platforms simplifying complex processes. MakerDAO, a notable example, manages the DAI stablecoin, pegged to the US dollar, through a system of smart contracts and overcollateralized debt positions (CDPs). Users mint DAI by depositing collateral, and the stability of DAI is maintained through a stability fee paid in MKR tokens.

MKR token holders play a crucial role in MakerDAO's governance, voting on system parameters like collateralization ratios and stability fees. The DAI Savings Rate (DSR) allows DAI

holders to earn interest, further supporting DAI's stability. Despite its robust design, MakerDAO faces risks such as market volatility and smart contract vulnerabilities. The mint and burn mechanism ensures DAIs value remains pegged to the US dollar by controlling its circulation based on market conditions. DAOs extend beyond financial protocols, encompassing various types such as collector, grants, impact, investment, media, product, protocol, service, and social/community DAOs (see Appendix C for further details). Examples include Pleasr DAO for collectors, Gitcoin for grants, KlimaDAO for impact, BitDAO for investments, and Bankless for media. These diverse applications highlight the versatility and potential of DAOs in the decentralized ecosystem.

4.1 Potential Risk Mechanisms

4.1.1 Early Identification of Potential Systemically Important DAOs and Protocols

Identifying successful Protocols and DAOs early on, before they reach critical mass in terms of adoption and locked value, can potentially help increase the detection and mitigation of systemic risks. If one is able to gather and analyze DAO statistics such as number of distinct members (liquidity fragmentation of governance token), vote proposal frequency and pass rate, member involvement and more, it may be possible to create a predictive model for successful DAOs. Note that 'successful' does not imply that the DAO's token gains in value, but rather that the organizational decision-making processes which the DAO implements lead to impact-generating outcomes for the protocol it governs and the ecosystem within which it is embedded. By creating 'digital twins' which are updated with sensor feeds from the environment, one can potentially study the impact of making quantitative changes to parameters and qualitative changes to mechanisms. Borrowing from machine learning training workflows, simulation update pipelines can turn a one-off model into a living, executable document which is continually updated to capture the emergent system behaviors throughout the protocol's lifecycle. Looking further down the road, it may become standard procedure for DAOs to actually operate their own off-chain digital twins, perhaps through a contracted service provider. It is interesting to think forward to a future where 3+ layers of zk-based (Zero-Knowledge) transaction compression might enable some or all of a model to be hosted on-chain.

4.1.2 Increasing Prevalence, Usage and Economic Impact

DAOs have the potential to revolutionize the employment model by allowing laborers to sell their skills more fluidly from day to day in a liquid labor market funded by DAO treasuries. With this potential future increased role as employers, hacks on DAOs could have more far reaching and possibly cascading effects depending on their size. If at some point in the future, a particular DAO employs 5000 people and that DAO's treasury is mismanaged and subsequently hacked, this could lead to an instantaneous economic shock in the form of a 5000-job loss.

Regardless of possible hacks of their smart contracts, DAOs may well become systemically important to what is viewed as the traditional economy, as alluded to above. They offer flexible and remote work opportunities and have the potential to create new job opportunities for workers and freelancers, offering more flexibility and the ability to work remotely. This can lead to an increased pool of talent, as geographical constraints are no longer a barrier to entry. Additionally,

the gig economy could benefit from the decentralized nature of DAOs, as it allows for more direct and efficient collaboration between workers and projects. DAOs also facilitate collaboration among individuals with diverse skills and expertise. This environment fosters knowledge sharing and learning opportunities for participants, helping them develop new skills and adapt to the ever-changing job market. Finally, as DAOs allow for decentralized decision-making, workers and freelancers can have more direct influence on the projects they are involved in. This can lead to a greater sense of ownership and motivation, potentially resulting in higher job satisfaction and productivity.

Take for example the largest Ethereum Layer 2 (L2) by total value locked (TVL), Arbitrum[14]. Arbitrum is completely DAO-controlled. On September 11, 2021, shortly after its permissionless mainnet launch, the TVL of Arbitrum was $238.85M. By June 6, 2024, TVL on Arbitrum had grown to $19.66B – nearly a 100x increase in less than three years. Only $5.78B of that TVL is the DAO's governance token, ARB, so these numbers represent a significant amount of value migration from mainnet or bridged from other L2s. In fact, Arbitrum's governance token's (ARB) marketcap peaked 2.5 months prior to the chain's TVL on March 23, 2024 at $6.78B, demonstrating that a DAO's token performance and ecosystem impact are not intrinsically coupled. Further, as more capital finds its way to Arbitrum and similar DAO-governed chains, such as Optimism, the potential economic impact of the bottom-up decision-making of these entities will only grow. Even more interesting is that DAO governance has had a major impact on this growth trajectory. For example, Arbitrum's Short-Term Incentive Program (STIP)[15] was a bottom-up initiative which provided ARB tokens from the DAO's treasury to Arbitrum-based protocols to use to grow their Daily Active User (DAU) and TVL metrics. It stands to reason that by adopting a decentralized methodology, i.e., deciding to distribute the decision-making around how to most effectively deliver stimulus, they effectively ramped their ecosystem and left the second-place L2 at the time (Optimism) in the dust[3]. Given the likely relevance of DAOs on tomorrow's economy, it may be prudent to investigate and research, among other topics, the possible regulatory landscape that could govern them, the concepts of job security and benefits as related to them and most importantly, the decision-making dynamics of their various governance structures which are currently quite a green-field set of experiments. As anyone who has become familiar with the concepts popularized by Balaji Srinivasan is his book, 'Network State', can surmise, we have only just begun to scratch the surface of the potential design space for cryptoeconomic-based systems of human coordination[16].

4.1.3 DAO and Protocol Governance Mechanics

While DAOs aim to achieve decentralized decision-making, there is the risk that a small number of large token holders or 'whales' could accumulate a majority of governance tokens. This could lead to centralization of power and decision-making, undermining the core principles of decentralization and potentially making the system more vulnerable to manipulation or malicious actions. Another risk, possibly tangentially related to the aforementioned "whale" risk, may come in the form of token holders prioritizing short-term gains over the long-term health and

[3]STIP was formally launched in September, 2023. At that time, Arbitrum's TVL was $6.48B and Optimism's was $2.76B. As of July 12, 2024, Arbitrum's TVL ($15.91B) is approximately $10B more than Optimism's ($5.99B).

sustainability of a protocol. This could lead to proposals being approved that have immediate financial benefits but might compromise the security or stability of the system in the long run. However, this risk may also be mitigated due to "whales" wanting to preserve their equity in the protocol/DAO by appealing to what the majority of voters (not necessarily token holders) would want.

While some DAOs are moving towards a more representative democracy model, rather than a direct democracy model, some DAOs may decide to keep a direct democracy model. A risk related to this type of governance mechanic is low voter participation. Many token holders may choose not to participate in the governance process due to a lack of interest, knowledge, or time. Low participation could result in important decisions being made by a small, unrepresentative group of token holders, which may not act in the best interests of the broader community. Furthermore, the open nature of DAO governance means that not all participants may have the necessary expertise to make informed decisions about complex protocol changes. This could lead to approval of proposals that may introduce unforeseen risks, vulnerabilities, or inefficiencies to the system.

In general, reaching consensus on proposals in a decentralized environment can be challenging, especially as the number of participants and the complexity of issues grow. Disagreements and prolonged debates over proposals can slow down decision-making and impede the ability of a protocol to adapt to changing market conditions or address emerging risks.

Finally, governance mechanics may expose a protocol to various attack vectors. For example, malicious actors could accumulate governance tokens to propose or approve actions that undermine the system or benefit them at the expense of others. Another potential attack is a 'governance rug pull', where developers or large token holders suddenly abandon the project after making decisions that negatively impact the protocol or its users.

4.1.4 Standards around DAO/Protocol Code, Parameterization, and Mechanism Diligence

Auditing smart contracts presents a big risk to the digital assets ecosystem as sometimes these examinations are done by a small number of people (maybe one or two people at some security firm like Slowmist etc...). Without a large (or at least larger) number of auditors, the smaller number may be more incentivized to keep a vulnerability they find hidden in order to exploit it later themselves rather than receive a much smaller bounty for finding the exploit[17]. As the number of auditors goes up, though, divulging the finding of a bug/possible exploit takes on dynamics of a prisoner's dilemma and auditors become more incentivized to collect the immediate bounty, lest some other auditor collects the bounty for the bug/exploit first. Places like Gauntlet have started escrowing some of their fee in case their parametric diligence didn't catch something, so why couldn't auditors do the same thing? This is all a matter of game theory and weighing risks and incentives and is an area worth exploring due to the vast amount of value that is currently locked up and even more so, due to the even more vast amounts of value that will likely be locked up in audited smart contracts in the future.

4.1.5 Mint/Burn Mechanisms/Design Patterns

Mint and burn mechanisms are fundamental processes in the Web3 ecosystem. They are used to manage a token economy by creating and destroying tokens to manage supply, and potentially token value, over the longer term. A loose analogy could be a central bank's monetary policy to increase or decrease currency in circulation.

The process of minting refers to creating new tokens that can represent various forms of value, such as fungible crypto and utility tokens or non-fungible tokens (NFTs), on a specific blockchain platform. Minting is typically governed by a rule set that may require multiple events to take place, such as smart contract and/or consensus mechanism triggers, that outline conditions for token creation to take place. Some common minting scenarios may include rewards for validating transactions and providing network security, fund raising events, and protocol governance.

Burning refers to permanently removing tokens from circulation by sending them to a designated smart contract that renders them irretrievable. Typically burning is done to manage token supply and price stability. Burning scenarios can take place at the transaction level by burning fees automatically, or at the organizational level by buying tokens at market and destroying them. Unused tokens from failed projects may also be burned to remove them from circulation.

Often protocols will increase buying pressure for their native tokens by implementing 'buyback-and-burn' techniques which use DAO-accrued value to conduct open-market token buying operations. These purchased tokens are then burned (i.e., sent to the 0x00 address) to remove them from circulation. Variants of this mechanism include 'buyback-and-make'[18], in which a protocol/DAO uses a private Balancer AMM pool to store the open-market purchased tokens. This has the same effect on structural flow but does not permanently reduce the circulating supply, nor does it burn the capital used to conduct the open market operations.

This delicate balance of minting and burning within a blockchain ecosystem, which composes traditional economics, game theory, and incentive design, has birthed the term "token engineering" to describe the financial and complex systems engineering required to create a sustainable and balanced ecosystem.

5 Risk Vulnerabilities in Decentralized Liquidity

One of the most prominent systemic risks in all of finance emerges from the absence of sufficient liquidity. From bank runs to stablecoin depegs, illiquidity is a significant factor.

Recommendation for Future Research

Explore mitigating systemic risk using liquidity-based intervention mechanisms, potentially secured by restaked digital assets, show promise as the 'Open Market Operations' of the future. This would most readily apply to regulated stablecoins. Could also be deployed against other DeFi 'critical infrastructure', such as ETH, e.g., if ETH is digital oil, then the U.S. may consider a strategic reserve. Caveat: restaked economic security comes with its own forms of systemic risk if stake is shared across protocols.

Recommendation for Future Research

Modeling and analysis of the dynamics of liquidity fragmentation to get 'left-of-boom' of liquidity-induced cascades

5.1 Potential Risk Mechanisms

5.1.1 Stablecoins

As shown in Section 1, relative liquidity balances dictate asset price according to the specifics of a pool and the AMM algorithm which governs it. For free-floating assets, even those paired against stablecoins, this approach to enabling price discovery is quite effective; shallower liquidity for a given asset pair simply leads to higher volatility.

However, the situation gets more complicated when dealing with the decentralized exchange of stablecoins themselves. When a stablecoin-stablecoin liquidity pool isn't perfectly in balance (which would mean there are no swaps occurring!), then one of the two assets is worth less than the other. Typically, such situations are arbitraged into alignment by market participants who are authorized to mint and redeem stablecoins, or others who are properly positioned to capture the premium between distinct markets.

The former type of participant will monitor the DEX stablecoin liquidity pools for discounted stablecoins, and purchase them as the dip below their peg. They then redeem those discounted stablecoins with the issuer for fiat at a 1:1 ratio, capturing the delta between the momentary market-discounted price and face value. Similarly, the latter type of participant will purchase the discounted stablecoin and then send it to another crypto market where full value is being offered. There are other, more complex methods of arbitrage, but sufficed to say, the decentralized set of arbitrage agents play a key role of ensuring stablecoins maintain their peg.

Stablecoins' reliance on emergent price equilibrium provides incredible resilience, but is not bulletproof. Let's explore some scenarios which lead to liquidity-induced systemic events; we'll focus specifically on stablecoin depegs, but these dynamics may present themselves in other markets as well.

Recommendation for Future Research

Investigate potential ways to boost confidence in stablecoins so they are not negatively affected by the traditional financial market's dynamics.

5.1.2 Confidence Impacts

Market participants must have confidence that the stablecoin they are buying at a discount has not experienced a catastrophic event which undermines the assumptions upon which it rests. If those assumptions are violated, there will be a run. A run will lead to stablecoin-stablecoin liquidity pool imbalances which are not arbitraged away. This is usually when the threshold is reached for what most market participants consider a depeg.

5.1.3 Temporal Impacts

A minor but sustained depeg in a single market may lead to other market participants to cease arbitraging away minor price fluctuations in other markets due to an increase in perceived risk, leading to a larger depeg occurring. This means that emergent liquidity conditions which are effectively random but disruptive to price stability may trigger the wider market to sell down to match them.

5.1.4 Regulatory Impacts

Regulatory intervention may have the unintended effect of disrupting liquidity flows which are vital to arbitrage operations. As an example, if a stablecoin's redemption function (i.e., the burning/redemption to fiat mechanism) were to be interrupted, a minor depeg event would likely occur. If this were to happen while a confidence-led depeg event was already ocurring, the depeg would become far more severe and longer-lasting, triggering temporal impacts across the wider ecosystem. On the other hand, regulatory signals related to liquidity-based intervention may have the effect of restoring market confidence and supporting a stablecoin's peg, as was seen during the Silicon Valley Bank run which temporarily caused a depeg in USDC.

5.1.5 Liquid Staking Tokens (LSTs)

Liquid staking tokens, such as the Lido DAO's STETH, represent a corresponding amount of staked Ethereum. These liquid wrappers enable the holder to use their staked Ethereum as collateral in various DeFi activities. While enabling composability of otherwise inaccessibly-locked liquidity, they present new vectors of systemic risk.

Imagine if the ETH underpinning a liquid staking token such as STETH gets slashed due to violations of the service provision guarantees, or worse, due to a software bug in the client software used to stake the underlying ETH. This would cause a run on STETH and result in a depeg of the STETH compared to the value of ETH.

5.1.6 Liquid Restaking Tokens (LRTs)

Liquid restaking tokens take another layer of risk beyond LSTs. In restaking, such as that found in the Eigenlayer protocol, a user commits their staked ETH to guarantee the provision of another service beyond the validation of the Ethereum network. If the expectations of performance of that additional service layer are violated, the ETH can be slashed to make the affected parties whole. In the LRT version of slashing, the staked ETH is automatically unstaked and awarded to the damaged party. The upside that draws users to provide liquidity to LRTs is the ability to earn additional yield on top of the yield provided by staking ETH to secure the Ethereum network.

The systemic risk that emerges from LRTs is from the Eigenlayer system architecture known as 'shared' or 'pooled' cryptpoeconomic security. This design increases the capital efficiency of the restaked ETH by enabling depositors to provide security for multiple 'Actively Validated Services' (AVSs) simultaneously to increase their yield. These AVSs payout a yield to the restakers who secure their services – this payment is then passed on to the LRT holders in the

form of new tokens (usually these are governance tokens for the LRT protocol), as is the case with LRT tokens such as EtherFi (ETHFI) and Renzo (REZ).

This systemic risk comes from the potential for a large shared security slashing event – if one were to occur, many AVSs could find themselves without adequate security. This would open them up to both malicious economic actors purposely misbehaving in order to capitalize on the inadequate security (imagine allowing oneself to be slashed in order to exfiltrate a large amount of value; that delta can be highly profitable) as well as a sudden run on the LRTs themselves, causing massively lost value for holders.

Further, if LRTs were to implode, likely there would be a lot of ETH dumped on the market, causing a significant cascade of value loss across the ecosystem.

Recommendation for Future Research

Given the incredible growth of TVL in LRTs, analysis and modeling of their fragility is needed to develop recommendations to increase their resilience to cascading events triggered by large failures in shared cryptoeconomic security pools while maintaining capital efficiency.

Recommendation for Future Research

Restaking shows much promise as a mechanism to secure any arbitrary service for any web/digital service/application – the increasing dependence must be met with stress testing and analysis.

5.1.7 Liquidity Fragmentation

Fragmentation of liquidity across multiple exchanges, products, or layer 2 scaling solutions (such as rollups) can lead to reduced market efficiency due to the lack of a unified order book[19]. Assets may trade at different prices across different venues, making price discovery more difficult and prone to price manipulation. Price manipulation can lead to cascading effects across multiple protocols and increase systemic risk within the entire crypto ecosystem.

Fragmented liquidity can also slow down the market's ability to respond to events or news, as the impact of such events takes longer to propagate through multiple platforms and ecosystems. This can result in a more sluggish and less resilient market, increasing the potential for systemic risks to build up and spread across the ecosystem.

Liquidity will continue to organically fragment across different users, protocols, exchanges, bridges, and Layer 2 solutions.

From a user experience perspective, users may need to interact with multiple platforms to access liquidity, increasing operational and counterparty risks, as users must manage multiple wallets, keys, and interfaces, increasing the likelihood of user errors or security breaches.

From an infrastructural perspective, if liquidity becomes more dispersed as the space grows, it may reduce overall scalability of the ecosystem and will contribute to systemic risk in the long run. Understanding these emergent phenomena in depth is challenging since many facets of the DeFi ecosystem are intertwined and rapidly evolving.

From a logical economic perspective, fragmented liquidity inevitably leads to shallow market depth, even in the most ubiquitous assets. The digital asset ecosystem relies on arbitrageurs to mitigate price dislocations, but as the infrastructural complexity increases, these agents' ability to source liquidity to arbitrage away dislocations caused by shallow markets may become slower. Temporally sustained dislocations may induce deeper markets to sell off. The crypto market is volatile enough; we must work to ensure that the friction created by infrastructural complexity does not exacerbate the systemic risk of the emergent dynamics of fragmented liquidity.

6 The Digital Asset Ecosystem as a Complex Adaptive System

As illustrated in the examples above, the web3 and DeFi ecosystem consist of a new class of interconnectivities and interdependencies between technological protocols and individual investor behaviors. Such sociotechnical systems are best analyzed within a Complex Adaptive Systems (CAS)[20][21][22][23] framework as they function through inductive, ground up mechanisms rather than top-down governance-based authorities.

In particular the underpinning of value in the DeFi ecosystem is the trustlessness that emerges from the interconnected set of individual decision-making agents who choose to participate in the system and come together to agree on the ground truth. The term trustless is often used to indicate a "lack of trust", however in the context of blockchain and digital ledgers, trustless refers to the property of not requiring trust of an intermediary to deliver specific functionality such as verifying and settling a transaction. This sociotechnical underpinning, which resides at the heart of the ecosystem, involves deep levels of interconnections between vast numbers of voluntarily participating entities. The scale and interconnectivity to produce the trustless properties required to remove intermediaries from execution, data availability, value transfer, and settlement is necessarily indicative of a complex system. For example, Ethereum, including its execution and data availability functions, is the result of a set of highly interconnected validators reaching consensus on each state transition.

User protection from a regulatory perspective must evolve to put in place rules which protect users from chain re-org-based challenges causing them to lose assets. To put a finer point on it, re-orgs can cause DeFi users to have much worse transaction outcomes via harmful Maximum Extractive Value (MEV). To be clear, not all MEV is bad MEV[24].

This complexity begets a number of regulatory challenges, as there is often no central executing entity to hold accountable. On the other hand, central control, when it does exist, can be easily obscured with a veil of complexity in front of it. The dynamic and permissionless nature of this complexity also means that ownership and control can change very rapidly. Regulatory concepts from TradFi, such as beneficial ownership, need to be upgraded to account for this new reality.

Furthermore, the DeFi ecosystem is adaptive at multiple scales; both the agents choosing to participate and the systems that arise from the set of agents participating are able to be changed. At the lower scale, agents are able to exit the ecosystem components that they no longer value. If enough agents believe that a given ecosystem component has drifted too far from its initial mission, then those agents will all choose to quit providing infrastructural support for that system, and that system will no longer be able to produce the properties required of it.

The digital asset ecosystem is composed of a constantly evolving set of protocols which co-adapt to one another at multiple scales.

This adaptive process can take place very quickly – even at a larger multiagent scale. As an example the founder of MakerDAO recently voiced support for an idea to fork Solana and transition Maker to a new Layer 1 chain[25]. Currently MakerDAO operates on the Ethereum mainnet. This is an excellent example of the extreme adaptation available to agents in this cross-chain ecosystem. If the DAO votes to approve this proposal, the entire underlying infrastructure of Maker will be remade from the ground up. There are many questions a user might want answered that no existing regulatory statute addresses, such as: How many nodes will this new chain consist of? Who will be controlling those nodes? What coin will be native to this chain (i.e., used for gas)? What enforcement mechanisms will be in place for malicious nodes? How will this transition take place in a trustless manner? If the majority of folks suddenly stop believing in the fundamental mission of a protocol, or stop believing that the protocol is fulfilling its obligation to achieve that mission, this fluid adaptivity can lead to what would be analogous to a 'bank run' on that protocol. This may become instantiated in the form of mass selling of that protocol's governance tokens with very little warning. It is also worth noting that the line between users and investors becomes very blurry, another challenge of adaptive digital economic systems which return value to those who use them.

Another characteristic of DeFi systems is the property of emergence; i.e. there are no singular entities or actors to which certain system operations can be ascribed. This is as true for Bitcoin as it is for Ethereum. Decentralized applications, although often initially developed by centralized entities, once deployed are executed by a decentralized network of computing power. Furthermore, it is typical for the mechanism to upgrade and change those contracts to also go through a process of progressive decentralization. This process often concludes with the launch of a governance token which enables its holders to propose and vote on changes to the associated protocol as well as the protocol's treasury management. As an example, consider Uniswap, whose core contracts are now permissionless and available to all in perpetuity. Uniswap Labs is constantly building new versions of the protocol and deploying them on-chain. Although there is a centralized team of core contributors, they only build upon the core protocol. That core protocol is controlled by a token-gated DAO. Future deployments of the Uniswap protocol (i.e., to new chains) are a matter of collective decision-making, an emergent process.

Approaches to mitigate systemic risk in digital asset ecosystems must at minimum take into account these foundational properties of trustlessness, multiscale adaptation, and emergence. Viewing these systems through a complex adaptive systems lens, we discuss elements of digital asset systemic risk analysis next.

7 Elements of Digital Asset Risk Analysis

Traditional macroeconomic analysis of stability is insufficient for understanding the complex dynamics of the crypto market. In particular, traditional macroeconomic analysis fails to account for the differing perspectives and information sets of various market participants. This traditional analysis focuses on, or at least assumes, the existence of centralized entities such as central banks, which exert a disproportionate amount of control over the system; this is not

the case in decentralized finance. For example, a fundamental economic analysis of a given crypto protocol would fail to account for bottom-up changes that can be initiated by any single agent in the system through a DAO proposal. In a publicly-traded TradFi company, operations and potential adaptations are not openly discussed on a public forum where any anonymous user can potentially spark a disruptive shift in the company's business model. The adaptive power of transparent operations and crowd-sourced intelligence and decision-making cannot be overstated.

Furthermore, there is both a temporal scale mismatch and an opacity assumption mismatch that limits the effectiveness of traditional regulatory controls, derived using traditional macroeconomic analysis, for blockchain based financial products and services. Quarterly risk disclosures are essential for opaque entities that require trust from owners and investors. In traditional financial markets, these disclosures serve as a mechanism for providing transparency and accountability. They help investors make informed decisions about the risks associated with their investments and ensure that companies operate within a framework of good corporate governance. The cycle time for entity-based regulatory compliance is significantly mismatched with the rapid pace at which the crypto market operates. Traditional regulatory frameworks rely on a slow OODA[26] (observe, orient, decide, and act) loop, which is inadequate to keep up with the fast-moving crypto ecosystem. This mismatch renders entity-based regulatory compliance almost entirely ineffective, as it fails to address the unique challenges and risks associated with the real-time dynamics of the crypto market. The crypto market is also characterized by a high degree of transparency, with most relevant system information, strategic decision processes, and tactical execution being publicly available. This transparency reduces the need for traditional risk disclosures in the crypto ecosystem, as the trustless nature of the technology allows for greater self-regulation by market forces.

To ensure proper alignment for the prevention of systemic risk, regulators must adapt their approaches to better fit the unique characteristics of the crypto ecosystem. Instead of relying solely on traditional entity-based regulation, they should consider adopting activity-based regulatory frameworks that account for the multiscale dynamics of the market and the diverse range of stakeholders involved. By doing so, they can foster a more resilient and transparent financial ecosystem that aligns with the principles of decentralization and trustlessness inherent in the crypto market.

To help develop such an activity-based approach, in the following list, we propose 8 essential elements of the digital asset ecosystem that must be taken into consideration:

1. **Interdependencies**: Traditional methods of risk analysis that are reductive in nature fail to consider the interdependencies that evolve between decentralized system participants. Typically, traditional risk analysis is entity-based, i.e., the risk to a given organization or asset is analyzed in a siloed and static manner. While this is often useful for making decisions around hedging particular assets, standard approaches do not consider the coevolutionary nature of systemic risk, where the whole is greater than the sum of the parts. The rapid evolution of the web3 ecosystem has made it apparent that the interdependencies among assets and participants must be considered. This need is not exclusive to DeFi but is also true for traditional finance. Take for example, the systemic risk that arose and was realized in 2008 due to mortgage-backed securities which bundled large

amounts of loans that were destined to default, and then sold them off to investors as yield-bearing assets. These investors then used them as leverage in other parts of the financial system. If liquidity is not readily available, then liquidations can have a catastrophic effect across the ecosystem, causing cascades of price crashes forcing selling causing more price crashes as unrelated leveraged positions are stressed by volatile clearing prices driven by low-liquidity conditions. Like a single match starting a thousand-acre forest fire, complex interconnected systems must be monitored and firewalled to stem contagion. Interestingly, these interdependencies are facilitated by decentralized protocols, and are then executed on-chain in a decentralized and trustless manner. As an analogy, consider TCP/IP's decentralized logical design. Each node/router makes a decision based on local information about where to forward each packet that hits it. Similarly, as each validator in the Ethereum blockchain makes a decision as to what to propose as the next block (if selected as the current leader), or the correctness of the next proposed block (if not the current leader), based on their own local perspective of the chain's tip and contents of the mempool (the highly dynamic set of unexecuted transactions). For new transactions to enter the mempool, they are broadcasted across the network. This means at any given moment, two geographically separated validators' perspectives of the state of the mempool will be different. If there were centralized orchestration mechanisms for TCP/IP packet routing or Ethereum mempool state, these technologies would likely be unable to reach the scale it which they currently operate. Further, if a node/router is dropped, the logical system continues to function as packets are routed around the issue by the decentralized decision-making of the other nodes/routers. Analogous to this is the negligible effect of an Ethereum validator going offline – the system doesn't miss a beat. Just as the cascading liquidations in TradFi took place over TCP/IP in 2008, cascading liquidations in DeFi take place over the credibly neutral, censorship resistant, guaranteed execution environment of Ethereum (which itself is built atop TCP/IP). Decentralization enables the emergence of interdependent cascades that cannot be halted in a top-down manner, as is done in the TradFi case when a limit-based circuit breaker halts trading in a highly volatile stock.

2. **Human Behavior**: Human behavior contributes significantly to systemic risk through contagion. In the crypto market, and free markets in general, the decisions and actions of individuals can create feedback loops that amplify volatility and increase the likelihood of cascading failure modes. In the case of DeFi lending markets, if a stablecoin was used as collateral for many loans, and that stablecoin underwent a loss of confidence event that was not rapidly mitigated, all of the loans would be liquidated automatically, and without negotiation or warning, further driving the failed stablecoin's price downwards. If the US government did not quickly decide to bail out the depositors of Silicon Valley Bank, for instance, then the USDC stablecoin might have never recovered from its temporary on-chain depeg. This hypothetical, more permanent depeg, may have triggered cascading liquidations across the ecosystem as USDC pervades DeFi protocols – both as collateral (market participants get liquidated) and as DAO treasuries reserves (DAO governance tokens crash as their treasuries' 'non-volatile' holdings suddenly nosedive in value). These tokens may be used in yet other DeFi protocols as collateral, causing the forest fire to continue to burn. We must increase focus and research to understand where in the web3

ecosystem we should erect constructive boundaries (i.e., firewalls for containing systemic risk contagion).

3. **Cyber & Economic Vulnerabilities**: The interconnectedness (interdependencies) and homogeneity of crypto networks may create systemic risk through shared cyber vulnerabilities. A cyber-attack or failure in one part of the system can have far-reaching consequences, potentially destabilizing the entire ecosystem. For a very simple, more cyber-focused example, not that there are multiple on-chain NFT marketplaces that leverage the OpenSea core contracts, such as Blur. If a vulnerability was discovered and exploited, the consequences may not be limited to one marketplace.

   A more nuanced example of the exploitation of an economic vulnerability could come in the form of the passing of a malicious governance proposal enabled by a flash loan. All token-vote DAOs with liquid governance tokens and fully on-chain governance processes (including fund distribution controlled by a technology such as Gnosis SafeSnap, which enables distribution execution autonomously and is usually considered a positive as it increases trustlessness). For an example of this, one can reference the Beanstalk DAO Attack, where that exact scenario played out. The Open Source Web3 Attack Reference (OSWAR) has classified this under "Privilege Escalation: 3. Governance exploit (DAO takeover)"[27]. Interestingly, this vulnerability is self-inflicted, as the exploit is actually a clever composition of individual web3 tools, each used as intended, but orchestrated in such a way as to raid the treasury of a protocol.

   Systemic cyber-economic vulnerabilities may be emergent in nature; that is, they are defined by the economic context within which they are situated. An example of a systemic cyber-economic vulnerability, which we may define as one in which a cyber-based exploit could result in an economic contagion, would be a susceptible cross-chain bridge which uses a lock and mint mechanism for value transfer. In these types of bridges, a native token is locked in a contract on one side of the bridge, and then what is known as a 'wrapped' version is minted on the far end. Sometimes, the bridge software on one chain is running a light client for the distal endpoint's chain, where a lock event is being listened for. When a valid lock event is detected on the distal chain, the corresponding wrapped token is minted on the near-side and sent to the appropriate address.

   Recommendation for Future Research

   Begin process of rigorous classification and creation of ontology related to all attack vectors and techniques[28] within this ecosystem[29], including, but not limited to novel cybersecurity attacks, but also exploits of an economic nature which are reliant on emergent properties from protocol execution and interactions (not necessarily cyber vulnerabilities).

   A now-infamous example of emergent economic vulnerability exploitation can be seen in the Mango Markets manipulation event, which was described in detail in the Potential Risk Mechanisms subsection of the Lending Protocol discussion above.

4. **Real-time Dynamics**: Digital asset products, services and protocols evolve at a fast pace,

in large part, due to the open-source nature of the web3 ecosystem; an ethos which allows development teams building in this space to quickly incorporate and build on improvements by various other ecosystem participants, who often, immediately make their innovations public and without any or many usage/licensing restrictions. This pace is only set to increase (possibly exponentially) with the introduction of mainstream artificial intelligence tools that can be used to multiply productivity.

5. **Distinguishing Speculators from Users**: To accurately assess systemic risk, it is crucial to differentiate between speculators and users in a given crypto community. These distinct groups have different risk appetites and contribute differently to emergent system dynamics. Further, some digital asset owners are not investors, but rather users who are required to possess a certain digital asset to access or pay for a service. Innovative new business models which return value directly to those who contribute to that value, without rent-seeking intermediaries, must be supported. If we do not find a way to be supportive while mitigating risk, we will only take on more risk in the long-term as less technically-qualified governments shape the ecosystem's evolution.

6. **Governance**:

   A) *Democratic, plutocratic, and hybrid control mechanisms; beneficial ownership*

      a) Protocols are most commonly controlled plutocratically via token-voting, with governance token accumulation being equivalent to control accumulation

      b) With decentralized ID (DID) approaches, democratic, i.e., one-human-one-vote mechanisms become possible; solutions such as Proof of Humanity[30] (PoH) have attempted to address this problem space with mixed results; without centralized ID attestations, such as a nation-state-managed database, these types of systems are susceptible to being gamed by motivated actors with the time and/or resources to execute duplicitous strategies. Non-blockchain-based approaches to DID such as Key Event Receipt Infrastructure (KERI)[31] may provide alternative solutions to achieving reliable on-chain democratic mechanisms; however successful integration of KERI with on-chain governance has yet to be demonstrated.

      c) Hybrid approaches such as quadratic voting[32], popularized by Gitcoin's grant awards process, also hold promise, but are subject to the same sybil-resistant reliability issues present with any DID-based governance mechanism

   B) *The risks of protocol governance are numerous:* As described above, democratic ownership of a protocol, while an excellent ideal to strive for to maintain decentralized control, is plagued by plutocratic realities. What this means is, those with the most capital to park (and the patience to park that capital at the most opportune times, i.e., a market downturn) are the ones who truly control the protocol. These risks are highly sensitive to initial conditions. For example, some protocols launch with very large insider allocations compared to others. This means that downstream, certain protocol creators may be the ones making decisions for the rest of the stakeholders and users, with one-token, one-vote power which dwarfs the average user's holdings.

Furthermore, there are a few central VC players in the ecosystem which have significant holdings in many of the largest protocols, so understanding beneficial ownership becomes a major challenge. To further complicate things, many of these protocols have delegatable voting power. For example, large amounts of a16z's UNI tokens are delegated to various University blockchain clubs, and these clubs sometimes make voting decisions which are not directly beneficial, and can even run counter, to a16z's overarching investment strategy. The risks engendered by plutocratic governance are challenging to confront.

C) *Dynamics of Control During a Protocol Governance Run - Often Initiated by a Governance Attack:* One of the risks that is amplified by plutocratic control is a run on a governance token. If a large amount of tokens are dumped on the open market by a single beneficial owner, it can ignite a panic to dump that token among all users. The ensuing downside price volatility could enable a malicious actor to buy up governance power at a significant discount to the value of the protocol's treasury, and follow-up by passing a malicious proposal to raid said treasury. TradFi has evolved regulatory solutions to this situation, going from the days of corporate raiding to what is now considered shareholder activism. It is critical that the regulatory and self-regulatory landscape for crypto evolve similarly in order to protect users. Direct application of TradFi concepts which assume a centralized control point for interdiction are not effective in the context of decentralized protocols. In terms of how this may mitigate systemic risk, in the event the protocol holds a significant amount of another protocol's token, then the prospect of those tokens being dumped can trigger a contagion event where the other protocol's tokens are dumped by the market in anticipation. If that protocol has intertwined interests with yet another protocol, a cascade may ensue. Evolving both bottom-up and regulatory-focused methods of protection against governance attacks are needed, just as has occurred historically in the TradFi context.

Recommendation for Future Research

Research if and how Corporate Raid defense regulations can be adapted in the context of DAOs. Research if and how DAOs can adapt the types of self-regulation that exist in TradFi in order to take proactive defensive postures against future governance attacks whilst leaving room for positive market-driven evolution which results from Shareholder Activism.

D) *Protocol Treasury Diversity:* Often, the bulk of a protocol's value held in their treasury, especially with immature protocols, is denominated in their own governance token. This lack of capital diversity can lead to extreme fragility of protocol value as feedback loops emerge between selling and protocol treasury valuation. As tokens are sold on the open market and the value of those tokens goes down, the intrinsic value of that DAO's treasury goes down with it, which further erodes the token's value as calculated by various market participants, which leads to more selling. This downward spiral, if left unchecked, may easily lead to complete value destruction of

a protocol.

7. **Treasury Deployment Aversion, i.e., Frontrunning by the DAO**: Another emergent dynamic which can bring about potential systemic risk in the world of crypto governance is the token holders not wanting to be front run by the DAO. In other words, if a DAO's treasury is mostly denominated in their native token, as mentioned above, any proposed deployment of capital in the service of increasing that protocol's resilience, either by swapping for other tokens in order to diversify holdings, or other expenditures such as funding the engagement of crypto-native modsim service providers to recommend parameter changes to actually reduce protocol risk (this is especially important for DeFi protocols operating amidst this dynamic landscape) is often meant with resistance by the token holders as they do not want the DAO to sell tokens on the open market to fund these operations as it will create sell pressure, at least temporarily. Another way to look at this is DAO governance token holders often fall victim to short-term thinking, choosing to forego actions that would lead to long-term stability for short-term value preservation. Often just the suggestion of such capital deployment can cause token holders to sell in anticipation. This short-term thinking serves to fragilize protocols and further exacerbate systemic risk to the ecosystem.

8. **Wisdom of the Crowd vs. Madness of the Crowd**: Although democratic protocol control which relies on the wisdom of the crowd may lead to more democratic outcomes, as well as creating unique investment opportunities for players unable to receive accreditation to 'get in on the ground floor', it also presents risks which can be summed up as the madness of the crowd – sometimes referred to as groupthink. Emergent, crowdsourced behavior is not a panacea, and governance mechanisms are at a very early stage of evolution. As a result, pathologically emergent decision-making, left unchecked, is a potential systemic risk to this ecosystem.

The following list describes the properties of the DeFi ecosystem which intrinsically may help mitigate systemic risk. Many of these inherent qualities of decentralized crypto infrastructure are drivers of the intense innovation and growth that this space has seen across academic, financial, and venture capital landscapes.

1. **On-Chain Transparency**: The open and transparent nature of blockchain enables anyone and everyone to have a real-time view of the ecosystem state. This inherent property has the effect of obviating the need for the type of data and disclosures historically provided by intermediaries in the traditional financial system, especially as they pertain to transaction execution and protocol governance. Additionally, some of most critical motivations for classifying investments as securities revolve around the opacity of investment contract operational execution. In other words, in the traditional financial system, a user holding an investment contract is unable to know for sure if their direct investment into a company (e.g., assume for instance a public company issues new shares into the market which happen to be purchased by a given user) is being used to fund capability and/or product growth, or to buy the founders a new private jet. Securities laws ensure that full

disclosure of company inputs and outputs are made available so abuse of public investment is deterred. In the DeFi ecosystem, many of those value flows are discoverable using a block explorer such as Etherscan. However, where transparency ends, regulation should likely begin.

Additionally, if realized systemic risk begins to propagate, the ecosystem participants are just as aware of it as anyone else, often allowing small problems to be widely recognized before they metastasize into large ones.

2. **Open-Source Software**: The open-source origin of most of the software deployed in the digital asset ecosystem, along with the publicly viewable bytecode of all migrated contracts, means that any and all potential eyes are able to observe systemic cyber vulnerabilities. This stands in stark contrast to the traditional financial system with its fully opaque operational systems that could be written using vulnerable software components or worse. That said, it is critical that diffusion of responsibility does not occur, and that careful auditing of open infrastructure is undertaken prior to it becoming systemically important.

3. **Permissionless Culture**: The permissionless ethos of web3 and DeFi engenders participation from the widest swath of diverse participants. As studies of CAS have taught us, diversity is a cornerstone of resilience, as homogeneous software implementations end up presenting systemic risk. For example, the Ethereum blockchain is composed of validator clients that all conform to the Ethereum specification, but there is no official Ethereum client release. From its inception, Ethereum's founders were adamant that diversity of implementation would be the network's strength, and metrics on client diversity are constantly in the spotlight. The reason is simple – if a vulnerability emerges on one client, there must be enough other clients that do not exhibit that vulnerability to keep the chain's liveness properties intact.

4. **Auction Markets**: The prevalence of auction markets for blockspace and transaction inclusion order are of paramount importance to the mitigation of systemic risk in this ecosystem. There are many auction markets at many scales of the ecosystem, and a discussion of them, and the reasons for their individual existence in detail, is far out of scope of this paper. However, speaking abstractly, auction markets ensure that transactions are ordered from the bottom up, which begets emergent functionality and bolsters systemic resilience when compared to the side effects of having a top-down approach to transaction execution.

5. **Maximum Extractable Value (MEV)**: Similar to auction markets, MEV is a source of systemic resilience in DeFi because it allows value to be extracted without force by those providing the value flow connections in the system networks, enabling the ecosystem to sustain itself from the bottom-up. However, we should caveat that on the other hand, MEV left unchecked most certainly presents a systemic risk as malicious forces could corrupt the system from the bottom up as well. As with all CAS, the rules of agent interaction must be carefully considered to avoid pathological emergence. Recent innovations coming out of the Ethereum research community are focused on providing means for MEV to be captured in-protocol. Examples include mechanisms such as Attestor-Proposer Separation

(APS-Burn)[33], i.e., Execution Auctions, which theoretically may reduce the systemic risk presented by MEV. APS-Burn and similar forward-looking designs have yet to be implemented and represent the cutting edge of open-source public blockchain R&D.

8 Conclusion: Developing A Complex Adaptive Systems Research Agenda

Tables 1-6 enumerate some of the common threads which are integral to the functioning and resilience of the digital assets ecosystem. While there are no hard lines between the described concepts and crypto examples (they could fit in more than one category), this provides a starting point from which to align future R&D efforts.

Emergence

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
What is the lack of an intermediary's effect on dynamics of truly emergent price volatility?	Asset Market Value[21]	Real-Time Dynamics
What drives emergent market confidence in given blockchains, assets, and institutions? What sorts of centralization does the market actually tolerate before confidence is eroded? How literal is "can't be evil > don't be evil" interpreted when market participants implicitly make confidence judgements?	Market Participant Confidence	Human behavior and incentives

Table 1: Complex Systems / Complexity Science Perspective: Emergence

Decentralized Decision-Making

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
How can we optimize DAO decision-making for increased reaction time?	DAO Governance	Cyber-Economic Vulnerability
How can we determine what information should be disclosed to users that is not on-chain or obvious?	User Protection	Opacity Assumption Mismatch
How can we provide layperson access to relevant information?	User Protection	Temporal Scale Mismatch
How can we provide automated & real-time disclosures?	User Protection	Cyber-Economic Vulnerability

'Decentralized in name only' fraud; How can we protect users from centralized systems that give the appearance of having decentralized control?	User Protection	Governance
How can we foster evolution beyond plutocratic mechanisms?	DAO Governance	Governance
How can we leverage decentralized ID to preserve privacy?	User Protection	Cyber-Economic Vulnerability
How can we incentivize and leverage frictionless collective intelligence?	Prediction Markets	Human behavior and incentives

Table 2: Complex Systems / Complexity Science Perspective: Decentralized Decision-Making

Interdependence vs. Interconnectivity

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
How can we reduce systemic risk introduced by bridges?	Bridges	Interdependencies
How can we advance evolution from locked asset bridges to message passing bridges to even less fragile future designs?	Bridges	Cyber-Economic Vulnerability
How can we address capital inefficiency of message passing bridges requiring dedicated liquidity on both sides?	Bridges	Cyber-Economic Vulnerability
How can we model depth of interdependence and emergent potential for systemic risk: e.g., stablecoin issued on one chain, bridged to another, then locked as collateral in a DeFi contract which emits a different asset that is bridged to a Layer 2 where it is added to a liquidity pool to farm rewards?	Bridges	Interdependencies
How can we increase the resilience of LSTs and LRTs with a shared security model to cascade-inducing tail-risk events?	Layer 1, 2 and Beyond	Interdependencies

Table 3: Complex Systems / Complexity Science Perspective: Interdependence vs. Interconnectivity

Multiscale Dynamics

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
How can we model feedback loops between layers?	Layer 1, 2 and Beyond	Real-time Dynamics
How can we study outcomes and fragility of interplay between individual agent decision-making and collective DAO decision-making, i.e., is a person who wants to vote against a proposal more likely to vote against it or just divest their stake (i.e., governance tokens)?	Voting in DAO vs. DAO taking actions	Human behavior and incentives
How can we address the systemic challenges of liquidity fragmentation and the infrastructural friction that can cause sustained price dislocations?	Layer 1, 2 and Beyond Distribution of LP across Chains, Protocols, and Users	Interdependencies Real-time Dynamics

Table 4: Complex Systems / Complexity Science Perspective: Multiscale Dynamics

Systemic Resilience and Elimination of Single Points of Failure, i.e., from hierarchy to swarm

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
How can we best model and stress test systemically important blockchain consensus algorithms to determine true fragility to attack?	Decentralized Chains PoW, PoS, etc.	Cyber-Economic Vulnerability
How can we best model and stress test protocols to determine if single points of failure exist (despite marketing of 'decentralization')?	DeFi Protocols	Interdependencies
How can we quantify decentralization of holdings, governance, and underlying infrastructure? and help layperson users understand how vulnerable a given token is?	Tokens	Cyber-Economic Vulnerability
How can we leverage the concept of restaked digital assets to secure liquidity-based interventions in times of systemic cascades?	Restaking, LRTs, Open Market Operations	Interdependencies

Table 5: Complex Systems / Complexity Science Perspective: Systemic Resilience and Elimination of Single Points of Failure

Bottom-Up Value Accrual

Potential Research Questions	**Digital Asset Ecosystem Applicability**	**Risk Area Addressed**
How can we get ahead of regulatory needs which will be driven by everyone and everything adopting economic properties? i.e., Friend.tech[34] allows anyone to tokenize themselves – malicious actors could theoretically open a synthetic short position on a person, censor or even harm that person, and derive profit	SocialFi (e.g., Friend.Tech)	Human behavior and incentives
How can we prevent MEV from becoming parasitic and systemically destructive?	APS-Burn / Execution Auctions	Human behavior and incentives

Table 6: Complex Systems / Complexity Science Perspective: Bottom-Up Value Accrual

In this whitepaper we have provided a comprehensive overview of some of the major subsystems of the digital asset ecosystem, together with a complex adaptive systems-based framing of its characteristics and functions. We further hypothesize that an activity-based regulation, which considers the multiscale dynamics of the crypto ecosystem, offers a more effective approach to systemic risk prevention, detection, and mitigation. By matching the temporal scale of the dynamics and the informational environment, regulators can develop more targeted and effective policies. Several research questions to help to better develop such an activities-based approach have also been proposed.

In closing we provide the following explicit call-to-actions to further help mitigate systemic risk in the web3 ecosystem:

- Increase focus and research to understand where in the web3 ecosystem we should erect constructive boundaries.
- Move from entity-based to an activity-based regulatory mindset; develop frameworks to begin to enact this change of perceptual frame.
- Building on the above, ensure parity with adversarial forces by constructing monitoring capabilities to ensure liquidity-based risks are understood before they become realized; all the data needed is open and available. More research must be done to know where exactly to find this data and how to use it.
- Understand the potential impacts of policy before it is enacted by implementing ecosystem modeling and simulation standards and best practices. Complexity science has paved a path that can be followed to undertake such a modeling task rigorously despite the

emergent functional nature of the ecosystem; such a process would have likely helped prevent 2008's mortgage-backed securities driven systemic event.

- Model systemic risk contagion propagation, potentially due to massive liquidation and deleveraging events; while most positions are overcollateralized now, this will likely change in the future as fractional reserve lending becomes more feasible. Modeling, and in turn, anticipating trigger events for systemic risk contagion propagation is important at the time of writing, but will become increasingly more important especially with the probable amplifying effects of such contagion due to fractional reserve lending/borrowing.
- Digital assets that become infrastructurally important to the U.S. economy would likely lead to the U.S. participating in said assets' security in order to increase national financial resiliency, as well as holding them in strategic reserve (i.e., BTC = > gold, ETH = > oil)[35]
  - Staking, mining, client development, consensus mechanism research

Appendices

Appendix A: Decentralized Exchanges and Liquidity Pools

Trading of crypto assets in the web3 ecosystem occurs on decentralized exchanges, colloquially known as DEXs. These exchanges are structured differently than their centralized, traditional counterparts which match buyers and sellers in a centralized order book. In the case of a decentralized exchange, a trader's order is not matched to other traders' orders, but rather, is executed by exchanging the token the trader wants to sell with the token they want to buy, within a liquidity pool containing both asset(s) of interest. Participants supply the liquidity pool with capital in the form of asset pairs to facilitate trades such as the one described above. These participants, known as liquidity providers, in turn, reap transaction fees for assuming the risks of providing the necessary liquidity.[36]

Within the context of a decentralized exchange, 'Liquidity pools' are smart contracts — self-executing computer programs — where the liquid capital is locked for the purpose of facilitating trade. Once capital is supplied by an individual, an Automated Market Maker (AMM) protocol powers the decentralized exchange between traders and liquidity pools such that there is no longer an intermediary.[37] While AMMs comprise the underlying mechanism powering all decentralized exchanges in the web3 ecosystem, they are not all created equally. Just as with traditional software, consumer demand and engineering resources have a large influence on the efficiency and safety of the codebase.

Trading fees are collected by the protocol for each execution and are typically split between the protocol itself and the liquidity pool(s). The fees kept by the protocol are usually held in protocol's associated Decentralized Autonomous Organization (DAO) treasury, another smart contract (see Section 3). Individual liquidity providers are awarded a portion of the total trading fees, proportional to the percentage of the pool's total liquidity that they are providing.

The main risk of providing liquidity to a liquidity pool is the concept of impermanent loss. Impermanent loss occurs when the relative price of the tokens supplied changes compared to when they were first deposited. This price change is a symptom of a shift in the underlying relative supply of the tokens in the pool. As tokens are usually supplied as a pair by liquidity providers, this shift causes the relative makeup of the liquidity provider's assets to also shift to reflect the liquidity pool's new token balance. Analogous terms could include unrealized opportunity cost, or, to a lesser extent, unrealized loss. The key to understanding impermanent loss is that one's deposits, and subsequent risks, are framed as a percentage of the ratio of the pool at the time of one's deposit action.

> *Example[a]: An ETH/BTC liquidity pool is programmed to keep the value of both baskets set at a 1:1 ratio. Alice supplies 20 ETH ($20,000) and 2 BTC ($20,000) –the current market rate– into a pool that is now 100 ETH ($100k) and 10 BTC ($100k) in size, constituting a 20% liquidity share.*
>
> *Two months later, the price of ETH doubles while BTC remains unchanged. As traders begin to arbitrage the liquidity pool to reflect the new market rates, the ratio of the pool decreases to 50 ETH ($100k) and 10 BTC ($100k), maintaining the value of both baskets at a 1:1 ratio.*
>
> *Alice's 20% deposit is now worth 10 ETH ($20,000) and 2 BTC ($20,000), which while still the same USD value, is 10 ETH less from her initial 20 ETH and 2 BTC deposit, resulting in an impermanent loss of 10 ETH. Had she simply kept her 20 ETH and 2 BTC in her personal custody, her token pair would be worth an extra $20,000.*
>
> *Alice's impermanent loss would become permanent should she withdraw her funds at the current market rates. However, there are two other considerations: Alice can keep her funds in the pool and continue to accrue transaction fees while waiting until prices revert to her original deposit ratio (not guaranteed).*
>
> *Alice may still be able to record a net profit even after taking the 10 ETH loss if the total transaction fees accrued are greater than 10 ETH.*

[a]This example is for illustrative purposes only and are not a one-size-fits-all design in the construction of a decentralized exchange or automated market maker protocol

The risks of impermanent loss are largely a function of volatility. The more volatile a token pair, the greater the risk of impermanent loss. One must do research to decide if the transaction fees that will be gained by providing liquidity for a particular token pair outweigh the potential risk of impermanent loss due to the assets' relative volatility. As discussed in subsequent sections, some protocols have added features over time to better utilize liquidity providers' capital such that the risk of impermanent loss becomes more muted (but not entirely eliminated).

A.1 Entity Example - Uniswap

Uniswap is a decentralized crypto exchange that operates on a number of blockchains, but most prominently on Ethereum. It uses smart contracts to conduct trades, enabling users to retain

full sovereign control of their assets while removing the need for trusted intermediaries and focusing on decentralization, censorship resistance, and security. Since its launch, Uniswap has gone through three major version updates, each with significant improvements to its operations. As of April 2023, it is the third largest crypto spot exchange globally, boasting a daily trading volume of around $1.2 billion.

Uniswap V1, launched in November 2018, provides an interface for the easy exchange of ERC20 tokens, built on the Ethereum blockchain. It is made up of ETH-ERC20 exchange contracts or 'liquidity pools'. If a token doesn't have an exchange, any user can create one, thanks to the open-source nature of Uniswap's codebase. Similarly to what is shown in Figure 1, below, A liquidity provider supplies an ETH/ERC-20 token pair to its designated liquidity pool, with each pool holding reserves of both ETH and its associated ERC20 token. An internal 'liquidity provider token' (LP token) is minted and sent to the provider's address, representing their contribution to the liquidity pool.

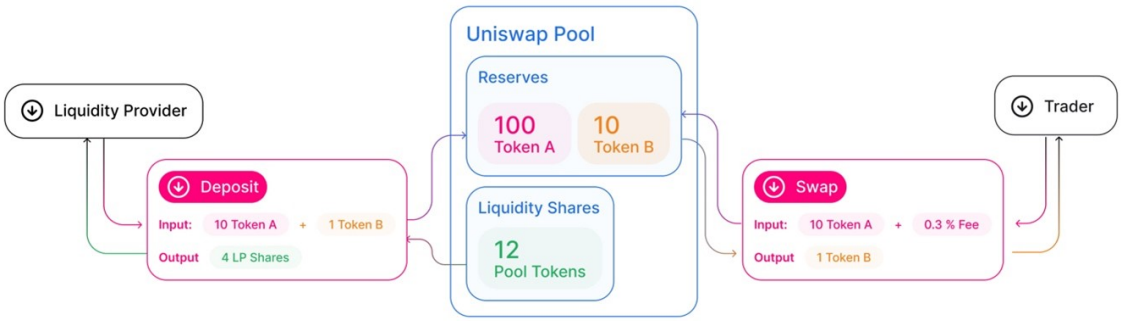

Figure 1: Uniswap Pool Description[38]

As shown above in Figure 2 and Figure 3 below, Uniswap V1 uses a 'constant product' formula for its Automated Market Maker smart contract, ensuring that trades do not alter the product of a pair's reserve balances. This formula guarantees that larger trades execute at exponentially worse rates than smaller ones, maintaining a balance within the system. The formula also sets the exchange rate based on the current size of reserves relative to the trader's order. After a trade is executed, a liquidity provider fee of 0.30% is taken and added to the liquidity pool's reserves, serving as the revenue center for the liquidity providers.

Uniswap V2 introduced several significant features, the most notable being the ability for liquidity providers to create pair contracts for any two ERC-20 tokens, rather than requiring ETH inclusion in a token pair as in V1[39]. This enhancement reduced trading fees and impermanent loss to liquidity providers. Additionally, V2 improved the price oracle by using the time-weighted average price (TWAP) of all trades in the previously mined block as the recorded price before transactions start populating a new block. Moreover, V2 introduced the concept of 'wrapped ETH' (WETH), an ERC-20 token representative of Ethereum's native asset, ETH.

Uniswap V3, launched in March 2021, introduced a novel Automated Market Maker system that introduces concentrated liquidity, which allows liquidity providers to choose a price

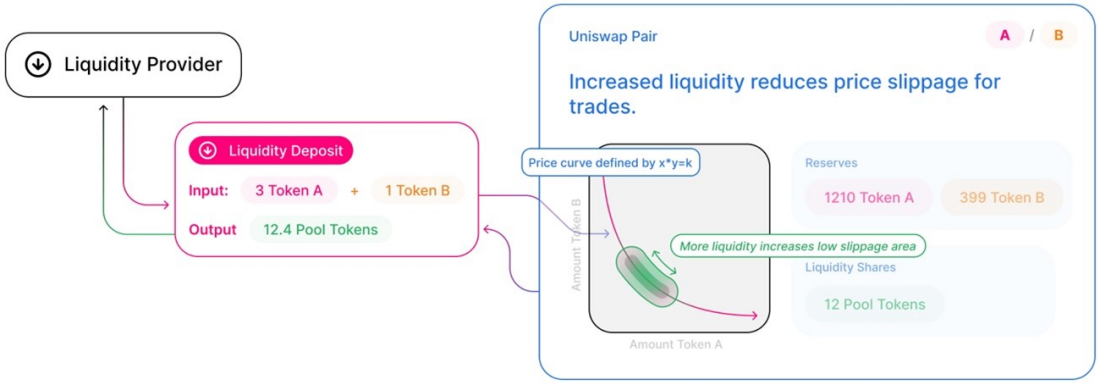

Figure 2: Price Curve of Uniswap Pool[38]

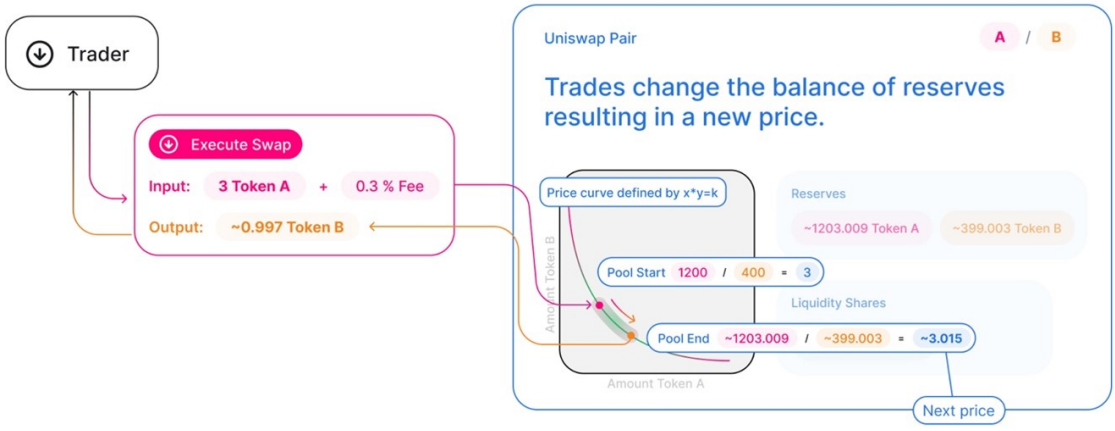

Figure 3: Dynamics of Price Curve[38]

range to deploy their capital while minimizing liquidity fragmentation and Ethereum gas fee inefficiency[40]. As shown in Figure 4 below, this new model allows for liquidity to concentrate around the mid-market price where most of the trading occurs and lets market forces determine where liquidity should be allocated in real-time.

However, Uniswap V3's changes have also led to a shift in the user base. The complexity of V3 and the need for strategic decision-making regarding liquidity provision, as shown in Figure 5 below, have meant that retail liquidity providers have been largely replaced by more capitalized professionals. These professionals possess the resources to develop sophisticated market-making and liquidity positioning strategies, creating a barrier to entry for less-experienced users. Nonetheless, Uniswap V3 has succeeded in implementing significant structural upgrades to its operating model, demonstrating the platform's continuous evolution.

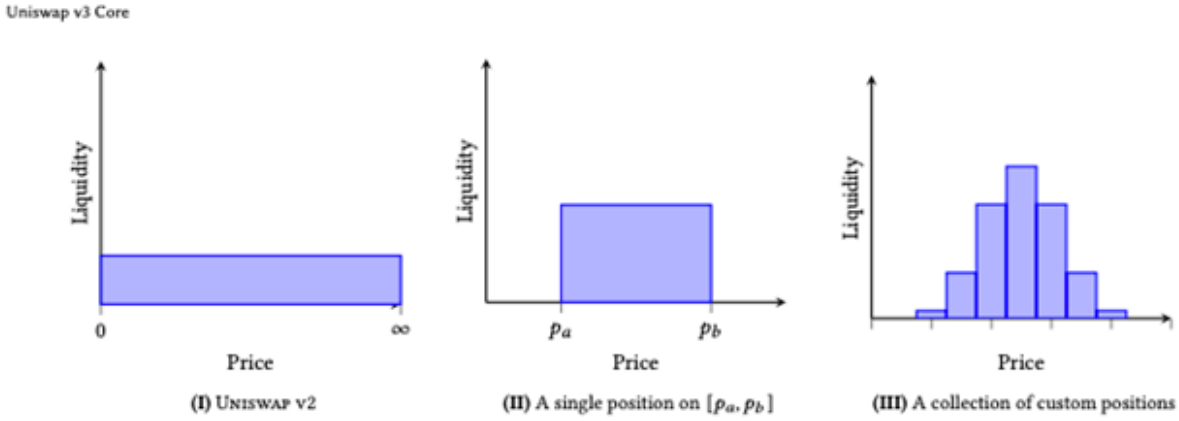

Figure 4: Liquidity Distributions in Uniswap Versions[40]

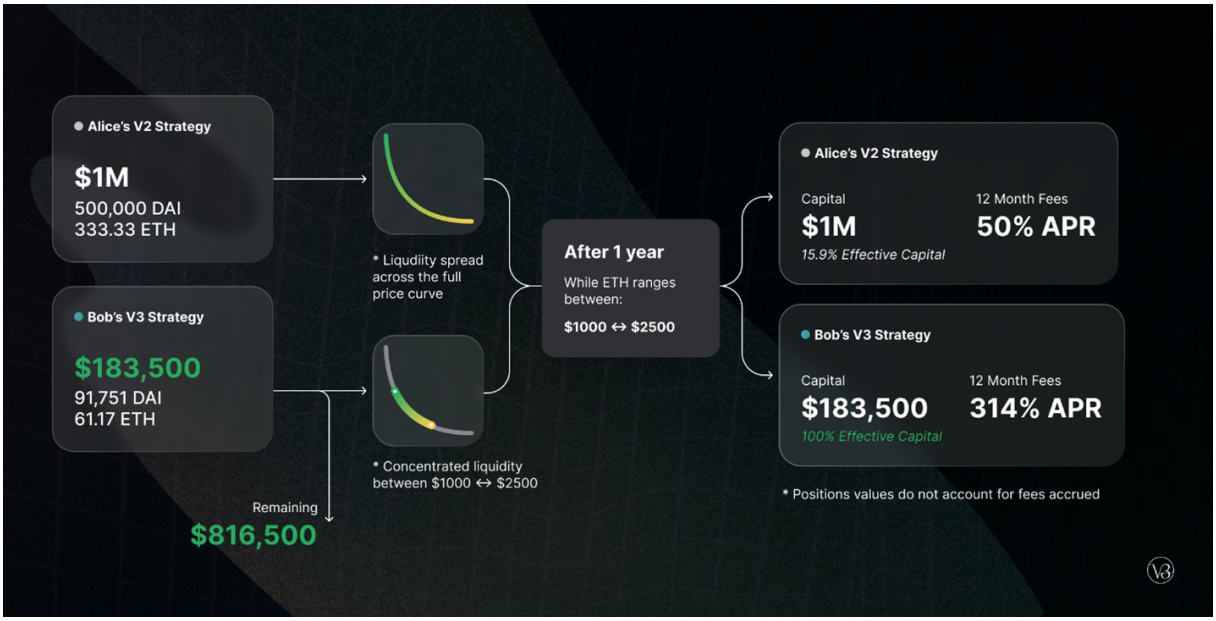

Figure 5: V2 liquidity provider vs V3 Liquidity provider[41]

A.1.1 Additional Agents and Protocols

- SushiSwap
- PancakeSwap
- GMX
- dydx
- DOPEX

Appendix B: Decentralized Money Markets and Lending

A decentralized money market serves a similar purpose as a traditional money market in that they both facilitate lending and borrowing of assets. However, there are several key differences between the two.

Like the traditional exchange in Section 1, a traditional money market relies on intermediaries in the form of banks or other financial institutions that facilitate lending and borrowing activities. In contrast, decentralized money markets have no intermediaries, and rely on smart contracts operating on blockchain platforms, to transact. Furthermore, accessibility is completely open to anyone with an internet connection and a digital wallet. There are no eligibility requirements or credit scores to lend or borrow; the caveat, with borrowing, being that loans in the space are generally required to be overcollateralized at this point in the technological development of the digital asset ecosystem.

An individual can supply assets to the money market/lending pool just as one would a traditional account, and the protocol utilizes the funds in the pool to make loans to would-be borrowers. This action is managed completely by a smart contract, nearly instantaneously. The smart contract is the lending pool. Traditional money markets on the other hand involve manual processes and potentially long settlement times. The individual agrees to an annual interest rate when they supply assets to the lending pool and the interest can be paid, depending on the protocol's code and the speed of new blocks on the protocol's blockchain platform.

> *Example: Alice wants to supply 100 ETH (approx. $150,000 USD) to a decentralized money market to earn 3% annually. The protocol pays interest every 15 seconds. Alice decides only after 1 minute she wants to withdraw her 100 ETH. Alice will have earned four interest payments of 1.43 x 10-6 ETH for a total interest accrued of 5.71 x 10-6ETH, or approx. $0.00856 USD over the one-minute period.*

Interest rates in a decentralized money market are driven purely by supply and demand algorithms or by the decision of a decentralized autonomous organization (DAO) which governs the lending pool. Since there is no intermediary and no central bank monetary policy affecting interest rate markets, it can provide clear and real-time insights into the market driven interest rate environment and be potentially more competitive for both lenders and borrowers.

From a borrower's perspective an individual simply needs to fulfill collateral obligations to secure a loan. Loans are typically overcollateralized in a decentralized money market, in part due to less information about the borrower and general volatility of current crypto markets. However, each protocol may utilize different algorithms to manage risk across its protocol/platform. Should the market rate for the borrower's collateral fall below a certain Loan-to-Value (LTV) threshold, the collateral is assumed by the protocol and liquidated. Each protocol uses slightly different techniques for acquiring external pricing and enforcing liquidation rules.

Example: Bob wishes to borrow $10,000 USDC (A US-Dollar backed token) against crypto he owns. The protocol determines the collateral factor for his crypto is 50% which implies Bob needs to collateralize $20,000 worth of his crypto for the 10,000 USDC he wishes to borrow. Bob locks up his collateral in a smart contract which accrues interest in the money market, while a second token is minted to act as a promissory note that calculates the loan amount and interest over time. When Bob is ready to pay back the loan, he supplies the promissory token with his current balance (loan balance + loan interest – collateral interest accrued) to unlock his initial collateral.

B.1 Entity Example – Compound

Compound Finance is a decentralized, autonomous, and open-source protocol built on the Ethereum blockchain. Compound enables users to lend and borrow digital assets without the need for intermediaries. The protocol employs smart contracts to manage pooled liquidity, interest rates, and user interactions. As of April 2023, the protocol manages approximately $750 million of open loans backed by $2.4 billion of collateral.

The Compound protocol was established in 2019 during a vibrant crypto market amongst maturing decentralized financial exchange mechanisms[42]. Some exchanges offered margin accounts, and peer to peer protocols existed to facilitate lending, but margin accounts contained centralization risk and limited user options, while peer-to-peer lending was asynchronously slow and costly. Most importantly, neither option was able to record transactions on–chain.

Compound's core infrastructure consists of a series of smart contracts that facilitate lending and borrowing without having to negotiate terms with a counterparty. These contracts create money markets for each supported asset, pooling liquidity from various sources, such as individual users, decentralized applications (dApps), and other protocols. Unlike the exchange and peer-to-peer examples, where lending is direct from one user to another, Compound aggregates the supply of each asset into pools, and each is treated as a fungible resource. By aggregating liquidity, the protocol ensures that users have access to a large pool of assets for borrowing and lending, improving overall capital efficiency.

Suppliers and borrowers interact directly with the protocol, earning or paying a floating interest rate. Interest rates on the platform are algorithmically determined, with each market having its own supply and borrow rates. Rates are influenced by the utilization ratio, which is the proportion of borrowed assets to the total supplied assets. When utilization increases, interest rates rise to incentivize more users to supply assets. Conversely, when utilization decreases, interest rates fall to encourage borrowing. The rates are updated with every transaction, and the value of a cToken's interest increases approximately every 12 seconds – the time it takes to validate an Ethereum block; cTokens are exchanged for underlying supplied asset to lending pool.[43]

When a user supplies an asset to a market, they receive a token balance in the form of an ERC-20 contract called a "cToken", which represents a claim to the underlying asset and any accrued interest. The cToken becomes convertible to an increasing amount of the underlying asset over time as interest accumulates, and users can monitor the cToken to track their earned interest. To withdraw assets, users can redeem their cTokens at the prevailing exchange rate

(underlying asset + accrued interest).

To borrow assets on Compound, users must first supply collateral in the form of one or more supported assets and be issued a cToken contract. The protocol checks the value(s) in the cToken(s), and if sufficient, will update the borrow balance in the cToken contract, and distribute the borrowed funds to the user's specified Ethereum wallet address. Each asset has its own collateral factor which determines the maximum borrowing capacity relative to the value of the supplied collateral. Collateral factors range from 0.00 to 1.00 (100%), with higher factors indicating lower risk and allowing for more significant borrowing capacity. For example, if a user supplies 1 ETH valued at $1,000 and the collateral factor is 0.5, the user can borrow $500 worth of any specified asset against the 1ETH collateral.

When a borrower is ready to pay back the loan and release collateral, the collateral minus the difference between borrowing costs from interest and the interest accrued while the collateral was supplied to the money market is returned to the borrower. It should be noted that a separate Ethereum gas fee must be paid for every transaction made from any protocol built on Ethereum such as Compound and is visibly included when performing any of the above transactions.

To ensure solvency, Compound requires borrowers to maintain a minimum level of collateralization, referred to as the account's health. The health factor is a ratio of the total supplied collateral value to the total borrowed value. If the health factor falls below a specified threshold due to market fluctuations, other users compete to liquidate the borrower's position, repaying the debt and earning a liquidation incentive in the process. It is the responsibility of the borrower to manage their account's health and add collateral if nearing the loan's liquidation threshold. Additionally, the borrower should have more than a cursory knowledge of finance and economics and be able to respond quickly to adverse events that directly affect the account health of the loan.

Compound is designed to be easily integrated into other DeFi applications and protocols. Developers can build upon Compound's infrastructure to create new products and services, such as yield farming strategies, leveraging borrowed assets, or creating tokenized investment portfolios. But as with any DeFi protocol, Compound is subject to risks, including smart contract vulnerabilities, economic exploits, and market volatility. To mitigate these risks, the protocol undergoes regular audits, maintains a bug bounty program, and employs security best practices.

B.1.1 Additional Agents and Protocols

- Aave
- Alchemix
- Liquity
- MakerDAO

Appendix C: Decentralized Autonomous Organizations (DAOs)

After understanding how powerful some of these protocols can be, a natural follow-up question may be, "how are these protocols are managed?". How are decisions made with relation to treasury management, product development, and hiring personnel? In the Web3/decentralized space, the community has the ultimate say in these decisions in the form of a Decentralized Autonomous Organization (DAO).

A DAO is a smart contract framework – a community-led entity – with no central authority. It lays the foundational governance rules, manages the treasury, and executes the decisions agreed upon by the community regarding the future of the project. Technical upgrades, treasury allocations, improvement proposals, and voting results are all managed by the DAO's publicly auditable smart contracts.

Typically, one becomes a community member by holding the governance token of a particular DAO. Community members' voting powers are proportional to their amount of governance token holdings. Along with voting rights, these DAO members can create proposals that serve to guide the DAO's/Project's trajectory. However, it should be noted that each DAO has different requirements for submitting a proposal. For example, if one wanted to create a proposal for the Curve Finance protocol, they would need to have 2,500 CRV ($2,500 USD) tokens locked within the protocol for four years, or 10,000 CRV ($10,000 USD) locked for one year, in order to do so. This key feature becomes an incentive mechanism for participants and helps weed out bad actors.

As mentioned in Sections 1 and 2, revenues generated for providing liquidity are often split between the liquidity providers and the protocol itself. In these cases, the protocol's cut of the revenue is effectively the DAO's revenue, since the DAO manages the protocol. Revenue can also be generated from, but not limited to, other transaction/service fees, token sales, membership fees, partnerships and sponsorships, and staking rewards.

The applicability of DAOs can extend much further than simply managing a protocol. DAOs can be set up to handle investments, grants, collectibles, services, social networks, and media. Other capabilities include designing novel voting mechanisms, raising capital, subDAOs (further codify operational responsibilities), and fractional ownership, to name a few. Additionally, tools like DAO creation platforms and DAO voting aggregators have been developed that serve simplify more complicated processes of certain protocols, thereby attracting more users to interact with these protocols within the DeFi ecosystem.

C.1 Entity Example - MakerDAO

C.1.1 Maker's Decentralized Autonomous Organization

MakerDAO, a decentralized autonomous organization (DAO) on the Ethereum blockchain, aims to establish a stable, decentralized digital currency known as DAI. Pegged to the US dollar, DAI strives to maintain a one-to-one value ratio with the USD, thereby serving as a medium of exchange, store of value, and unit of account. This reduces the price volatility usually seen with cryptocurrencies.

MakerDAO's system is driven by a set of smart contracts that manage the creation and stability of DAI. Users can create DAI by depositing collateral, such as Ether or other cryp-

tocurrencies, into a collateralized debt position (CDP). The CDP, a smart contract, secures the collateral and mints an equivalent DAI amount determined by the value of the collateral and a required collateralization ratio. This ratio ensures DAI's overcollateralization, where the collateral's value surpasses that of the created DAI, thereby providing a buffer against collateral value fluctuations and preserving DAI's stability. If the collateral's value drops below the required ratio, the CDP can be liquidated, selling the collateral to cover the DAI debt.

DAI's stability is further maintained through a stability fee which is calculated using a variable annual percentage fee that accrues continuously on the outstanding DAI debt in a vault. The fee must be paid when closing a vault or repaying DAI debt. This fee can be paid in MKR, MakerDAO's governance token, which encourages users to repay their DAI debt. The stability fee can be adjusted by MKR token holders to influence DAI's supply and demand, thus maintaining its peg to the US dollar. When DAI price is below $1, the stability fee may be increased to reduce DAI supply and boost the price. When DAI is above $1, the fee may be decreased to increase the supply of DAI.

MKR tokens have a pivotal role in MakerDAO's governance. MKR holders can vote on proposals to change system parameters like collateralization ratios, stability fees, supported collateral types, and debt ceilings. Their participation in governance helps shape the direction of MakerDAO, thus ensuring DAI's long-term stability and growth. Additionally, there's the DAI Savings Rate (DSR) token, another MakerDAO token, that allows DAI holders to lock their tokens into the DSR contract and earn interest over time. This mechanism supports DAI's stability by encouraging users to lock up their DAI, potentially increasing demand.

While MakerDAO's decentralized governance model and overcollateralization make it a strong and reliable platform for a stable digital currency, it's not entirely risk-free. Potential threats include market volatility, smart contract vulnerabilities, and regulatory challenges. Nevertheless, MakerDAO is an innovative and accessible DAO that uses smart contracts, tokenized governance, and financial incentives to create a stable, decentralized digital currency, making it an excellent study case for those new to DAOs in the DeFi space.

C.1.2 Additional DAOs

DAO Type	**DAO Examples**
Collector	Pleasr DAO
Grants	Gitcoin, Uniswap, Bankless, AAVE Grants DAO, Big Green DAO
Impact	KlimaDAO, Human DAO, Golden DAO
Investment	BitDAO, MetaCartel Ventures, People DAO
Media	Bankless, Decrypt
Product	The Graph, Sushi, Decentraland
Protocol	MakerDAO, Uniswap, Yearn.Finance
Service	The Graph, PoolTogether
Social/Community	Developer DAO

Table 7: Other Types of DAOs and Examples

Acknowledgments

We thank Scott Rosen and Colin Van Oort for their constructive feedback.

References

[1] Krisztian Sandor and Ekin Genç. *The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA*. Updated April 14, 2024. CoinDesk. July 2022. URL: https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/.

[2] Timothy Smith. *What Was FTX? An Overview of the Exchange*. Investopedia. June 2024. URL: https://www.investopedia.com/ftx-exchange-5200842.

[3] Arijit Sarkar. *USDC depegs as Circle confirms $3.3B stuck with Silicon Valley Bank*. Cointelegraph. Mar. 2023. URL: https://cointelegraph.com/news/usdc-depegs-as-circle-confirms-3-3b-stuck-with-silicon-valley-bank.

[4] Wikipedia contributors. *Collapse of Silicon Valley Bank*. Updated April 17, 2024. Wikipedia. Mar. 2023.

[5] Wikipedia contributors. *Complex system*. Updated July 28, 2024. Wikipedia. May 2011.

[6] Solidus Labs. *The Mango Exploit: An Order Book Analysis*. Solids Labs. Oct. 2022. URL: https://www.soliduslabs.com/post/mango-hack.

[7] Edward Helmore. *USD Coin depeg: Silicon Valley Bank collapse*. The Guardian. Mar. 2023. URL: https://www.theguardian.com/technology/2023/mar/11/usd-coin-depeg-silicon-valley-bank-collapse.

[8] Suzanne O'Halloran. *Bitcoin ETF Blowout Wows Even BlackRock's Larry Fink*. Fox Business. Mar. 2024. URL: https://www.foxbusiness.com/markets/bitcoin-etf-blowout-wows-even-blackrocks-larry-fink.

[9] Alexandra Andhov. *Ethereum ETFs Approved: Insights into the SEC's Decision*. Updated May 24, 2024. Forbes. May 2024. URL: https://www.forbes.com/sites/digital-assets/2024/05/23/ethereum-etfs-approved-insights-into-the-secs-decision.

[10] Jen Wieczner. *Barney Frank Says More Shuttering Signature Bank*. New York Magazine. Mar. 2023. URL: https://nymag.com/intelligencer/2023/03/barney-frank-says-more-shuttering-signature-bank.html.

[11] Denis — MISO. *On Insolvency: Tackling Bad Debt in DeFi*. Sept. 2022. URL: https://medium.com/risk-dao/on-insolvency-tackling-bad-debt-in-defi-6c2ac5028348.

[12] David Siegel. *Understanding the DAO Attack*. Updated January 13, 2023. CoinDesk. June 2016. URL: https://www.coindesk.com/learn/understanding-the-dao-attack/.

[13] Cheyenne Ligon. *Mango Markets Exploiter Avi Eisenberg Found Guilty of Fraud and Manipulation*. Updated April 18, 2023. CoinDesk. Apr. 2024. URL: https://www.coindesk.com/policy/2024/04/18/mango-markets-exploiter-avi-eisenberg-found-guilty-of-fraud-and-manipulation/.

[14] *Arbitrum One*. L2BEAT. URL: https://l2beat.com/scaling/projects/arbitrum.

[15] tnorm. *How to Apply: Arbitrum Short Term Incentives Program*. Arbitrum Foundation. Sept. 2023. URL: https://forum.arbitrum.foundation/t/how-to-apply-arbitrum-short-term-incentives-program/16545.

[16] Alexandra Mccarroll. *Crypto Social Experiments: A Beginner's Guide to Network States and Vitalik Buterin's Initiative in Montenegro*. Updated October 23, 2023. Forbes. May 2023. URL: https://www.forbes.com/sites/alexandramccarroll/2023/05/26/crypto-social-experiments-a-beginners-guide-to-network-states-and-vitalik-buterins-initiative-in-montenegro/.

[17] Nick Almond. *(audit, audit)*. May 2022. URL: https://thecryptospace.substack.com/p/audit-audit?s=w.

[18] Joel Monegro. *Stop Burning Tokens - Buyback and Make Instead*. Placeholder VC. Sept. 2020. URL: https://www.placeholder.vc/blog/2020/9/17/stop-burning-tokens-buyback-and-make-instead.

[19] Javier Martin Diaz. *Mastering the Layer 2 Landscape: A Guide to Ethereum Scaling Solutions, Challenges, and Risks*. Aug. 2023. URL: https://blog.summer.fi/mastering-the-layer-2-landscape-a-guide-to-ethereum-scaling-solutions-challenges-and-risks/.

[20] P. W. Anderson. "More is different: broken symmetry and the nature of the hierarchical structure of science". In: *Science* 177.4047 (1972), pp. 393–396. URL: https://doi.org/10.1126/science.177.4047.393.

[21] M. D. Norman, Y. G. Karavas, and H. Reed. "The Emergence of Trust and Value in Public Blockchain Networks". In: *IX International Conference on Complex Systems* (July 2018), p. 22. URL: https://www.researchgate.net/profile/Michael-Norman/publication/325552991_The_Emergence_of_Trust_and_Value_in_Public_Blockchain_Networks/links/5b158ad74585151f91fafbba/The-Emergence-of-Trust-and-Value-in-Public-Blockchain-Networks.pdf.

[22] Wikipedia contributors. *Complex adaptive system*. Updated July 28, 2024. Wikipedia. May 2005.

[23] J. H. Holland. "Complex adaptive systems". In: *Daedalus* 121.1 (1992), pp. 17–30.

[24] Corwin Smith Nico jakoooob Joseph Cook Pablo Pettinari Ahmed Ali Eridian Joshua Emmanuel Awosika Hursit Tarcan Open Source Paul Wackerow Marius Kjærstad. *Maximal extractable value (MEV)*. Updated July 3, 2024. Built on Github via Open Source Contributions. Ethereum Foundation. July 2024. URL: https://ethereum.org/en/developers/docs/mev/.

[25] Brian Quarmby. *Maker DAO Co-founder Proposes Solana Codebase Fork Native Chain*. Cointelegraph. Sept. 2023. URL: https://cointelegraph.com/news/maker-dao-co-founder-proposes-solana-codebase-fork-native-chain.

[26] Col. John R. Boyd. *A Discourse on Winning and Losing*. Air University Press, 2018, 1987. Chap. Organic design for command and control, pp. 218–253. URL: https://www.coljohnboyd.com/static/documents/2018-03__Boyd_John_R__edited_Hammond_Grant_T__A_Discourse_on_Winning_and_Losing.pdf.

[27] Open Source. *Governance exploit (DAO takeover)*. Built on Github via Open Source Contributions. OSWAR. URL: https://www.oswar.org/attack/70.

[28] The MITRE Corporation. *MITRE ATT&CK Matrix for Enterprise*. The MITRE Corporation. URL: https://attack.mitre.org/.

[29] Open Source. *OSWAR - Open Standard Web3 Attack Reference*. OSWAR. URL: https://www.oswar.org/#oswar.

[30] *The Internet of Humans*. Proof of Humanity. URL: https://proofofhumanity.id/.

[31] Open Source. *KERI Glossary*. Built on Github via Open Source Contributions. Identity Foundation. URL: https://identity.foundation/keri/docs/Glossary.html.

[32] Mashal Waqar. *Quadratic Voting: A How-to Guide*. Gitcoin. URL: https://www.gitcoin.co/blog/quadratic-voting-a-how-to-guide.

[33] barnabe.eth. *More pictures about proposers and builders*. Apr. 2024. URL: https://mirror.xyz/barnabe.eth/QJ6W0mmyOwjec-2zuH6lZb0iEI2aYFB9gE-LHWIMzjQ.

[34] friend.tech. *friend.tech Homepage*. friend.tech. URL: https://www.friend.tech/.

[35] Jalpa Bhavsar. *Trump to Announce Bitcoin as US Strategic Asset at Conference*. Updated July 19, 2024. The Crypto Times. July 2024. URL: https://www.cryptotimes.io/2024/07/18/trump-to-announce-bitcoin-as-us-strategic-asset-at-conference/.

[36] Cryptopedia Staff. *What Are Liquidity Pools?* Updated November 16, 2023. Gemini/Cryptopedia. Nov. 2023. URL: https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity.

[37] Cryptopedia Staff. *What Are Automated Market Makers (AMM)?* Updated October 2, 2023. Gemini/Cryptopedia. Oct. 2023. URL: https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers.

[38] Uniswap Foundation/Open-Source. *How Uniswap works*. Uniswap Foundation. URL: https://docs.uniswap.org/contracts/v2/concepts/protocol-overview/how-uniswap-works.

[39] Dan Robinson Hayden Adams Noah Zinsmeister. "Uniswap v2 Core". In: *Uniswap Foundation* (Mar. 2020). URL: https://docs.uniswap.org/whitepaper.pdf.

[40] Moody Salem River Keefer Dan Robinson Hayden Adams Noah Zinsmeister. "Uniswap v3 Core". In: *Uniswap Foundation* (Mar. 2021). URL: https://uniswap.org/whitepaper-v3.pdf.

[41] Uniswap Team. *Introducing Uniswap v3*. Updated March 23, 2023. Mar. 2023. URL: https://blog.uniswap.org/uniswap-v3.

[42] Geoffrey Hayes Robert Leshner. "Compound: The Money Market Protocol". In: (Feb. 2019). URL: https://compound.finance/documents/Compound.Whitepaper.pdf.

[43] IvanOnTech. *The Ultimate Guide to Compound's cTokens*. Updated June 22, 2021. Moralis. June 2021. URL: https://academy.moralis.io/blog/the-ultimate-guide-to-compounds-ctokens.