GOVERNANCE ANALYSIS OF DECENTRALIZED EXCHANGE APPLICATIONS

An institutional economics approach

TU Delft

GIANMARCO FERRARI

This page was intentionally left blank.

Governance analysis of decentralized exchange applications

An institutional economics approach

by

Gianmarco Ferrari

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on March 28th, 2022.

Student number:	4489314	
Project duration:	October 27, 2020 - March 28, 2022	
Thesis committee:	Dr. ir. Rutger van Bergem	TU Delft, Advisor
	Dr. ir. Bert Enserink	TU Delft, Supervisor
	Dr. Aad Correlje	TU Delft, Chairman

An electronic version of this thesis is available at http://repository.tudelft.nl/.

This page was intentionally left blank.

Acknowledgements

The following report contains my research on the new institutional frontiers allowed by blockchain technology, the final deliverable for the degree of Master of Science in Engineering and Policy Analysis. Though I stand as the sole author of this thesis, its completion would not have been possible without the help of certain people whom I would like to thank.

First, I would like to thank my three supervisors Dr. Bert Enserink, Dr. Aad Correlje and Dr. Rutger van Bergem. Bert for the strong support and guidance provided during the entire duration of the research. Aad for your valuable theoretical inputs and for guiding me in thoughtful reflections on my work. Rutger, for countless hours spent discussing research, blockchain, its societal implications and life in general. I owe to you most of my learnings of this period of my life, for this I will forever be grateful.

I am particularly grateful to Agnese, for the endless moral support through highs and lows. For proving that your patience barely has any limit. For your technical support, and for your irrational and sweet love which makes any setback less bitter and every accomplishment more worth living.

To Val, for gifting me with true and incorruptible friendship that has eased this journey in so many occasions. To Nikhil, for teaching me that not taking yourself too seriously is an actual life hack. To Lex, for the unthinkable experiences we have shared through thin and thick. To Andrei, for always being firmly present in times of need and for your remarkable intellectual honesty.

Finally, I would like to wholeheartedly thank my family. Pina, Walter and Maria Francesca. This achievement has been made possible in no small part by your constant love and support throughout the years. To say I am lucky to have you is a significant understatement. I am forever grateful for the opportunities you have allowed me to have.

Gianmarco Ferrari
Delft, March 2022

Contents

List of Figures

List of Tables

This page was intentionally left blank.

Executive Summary

Blockchain technology has introduced the possibility to exchange value and information through the internet without the supervision or permission from any third party intermediary. While many private and public entities have seen this as a chance to increase their operational efficiency, other ventures have been utilizing this same edge as a mean to develop new institutional regimes given the impact on transaction cost reduction,

The theories central to institutional economics claim that transaction costs are the ultimate driver for shifts in institutional settings. The purpose of the following research was to investigate whether the reduction in transaction costs allowed by blockchain technology is effectively causing new forms of institutions to arise. Given that blockchain is still in its infancy, there is a current lack of academic literature addressing its governance edge. Furthermore, the few studies available adopt a comparative approach, hence failing to explore the entirety of new institutional possibilities. For this reason, the following research utilized the Institutional Analysis and development framework developed by Elinor Ostrom as a holistic and institutional agnostic method of analysis.

The particular application analyzed was the one of financial product exchanges. Today, the exchange of financial products as securities, is coordinated by hierarchical organizations, namely firms. As a matter of fact, multiple different firms are involved in the exchange of these products. Exchanges are responsible for matching buyers and sellers, clearing houses assume counter party risks and make sure the trading parties can meet their obligations, and custodians and central security depositories are responsible for the final settlement of transactions. Furthermore, reconciliation costs are incurred by all participants when updating their respective databases. Given that blockchains are fundamentally public distributed records of transaction, they effectively undermine the economic efficiency and logic of the current systems of clearing, settlement and reconciliation. Decentralized exchanges are tackling these issues today.

For the purpose of the analysis a total of three decentralized exchanges were shortlisted from the over 200 existing. The first filter of choice was to choose between exchanges native to the Ethereum blockchain. This because, being the oldest in the space, they present the most well developed and resilient communities apt for the analysis. Next, exchanges were further filtered by total liquidity in the protocol, or total value locked, and trading volume. The three exchanges selected for the analysis in the end were Uniswap, Sushiswap and Curve. Given that these protocols run on a public and permissionless blockchain, it was possible to retrieve large amounts of data on their relative performance. A number of data acquisition and analytics platforms were utilized for data analysis and visualization namely, Dune, Tally and Sybil.

The implementation of the Institutional Analysis and Development framework showed that of all the rules in use, boundary and payoff rules are the ones that have major impact on the behaviour of the community and the performance of the protocol itself. In particular, the protocols with the most sophisticated incentive and deterrent schemes are the ones that manage to attract more users, hence capital. All protocols utilize governance tokens in order to distribute governance rights (voting and proposing), and most of them use a one token one vote model. However, these models result in power centralization due token accumulation. In fact, all project analyzed displayed high levels of both decision making power centralization and voter apathy.

While the latter can be a result of the former, it could also be a result of the high technical knowledge required in order to participate in governance.

The analysis also displayed that each project adopts a different interpretation of governance. This becomes apparent by utilizing the vertical approach to rule analysis developed by Ostrom. For instance, Curve only allows the community to decide on operational features of the protocol as adding new liquidity pools or fee bases. Uniswap, also allows for voting on the decision making process itself, as changing the quorum threshold for proposals to pass. Finally, Sushiswap allows the community to even vote on who should be part of the core management team of the protocol. This shows how at this early stage of development there is no consistency in the study and design of governance.

While one of the main tenets of the applications built on blockchains is to decentralize both its operations and governance, for the time being only the former is true. As a matter of fact, at the current stage of development, the governance of decentralized applications are more resembling hierarchical coordination systems and corporate governance in particular, where most decisions concerning the strategy and main operations of the protocol are taken by a small set of individuals. However, there are some signs that reveal new institutional regimes are forming. For instance, the development of new voting systems which manage to gauge the commitment and consistency of governance participants, as new token distribution mechanisms that try to prevent some players from having excessive amount of voting power with respect to others. In conclusion, as predicted by Coase, the reduction of transaction costs is effectively shifting institutional regimes. It may just be too early for it to be apparent.

1 Introduction

In early 2009, after decades of trial and error, a group of mostly computer scientists and cryptographers, or 'cypherpunks' (May, 1988), finally managed to deploy a software able to securely execute and record transactions on a decentralized ledger. Given its technical specifications, this new technology was later defined as 'blockchain' (Nakamoto, 2009). Blockchains leverage cryptography, computational power and game theory to create a network where participants can safely exchange value and information without the supervision nor coordination from any third-party intermediary. As any new technology yet in its embryonic phase of development, it's true potential is still to be fully understood and explored. Nonetheless, in the span of slightly more than a decade, the space has grown and evolved faster than any other innovation has ever achieved, such that governments and private sector organizations (from tech companies to financial institutions) are currently being deeply involved in researching in the field (Auer and Böhme, 2020).

Fundamentally, blockchains have a varied set of attributes. In a way they create new digital payment rails. In other words, an alternative and more efficient form for exchanging value through the internet. This of course, makes it a direct competitor to existing global payment rails as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and the Single Euro Payments Area (SEPA) in Europe. As a matter of fact, remittance has been among the first and most adopted use cases, particularly in developing countries. Nevertheless, blockchains do more than that. For instance, another attribute is the ability to create digital scarcity. This means that of any digital asset deployed on a blockchain, only a certain predefined quantity can be programmed to exist. A good example for this is Bitcoin, of which only 21 million units can ever exist (Nakamoto, 2009). The underlying immutable and decentralized ledger is also meant to guarantee and validate such scarcity. On the other hand, tokenization is the concept of being able to represent on a blockchain any real world asset, whether physical as commodities and real estate or non tangible as intellectual property (Tian et al., 2020). Therefore, tokenization can be seen as the process of replicating real world scarcity into digital scarcity.

With all this being said, one can now understand that the digital payment rails facilitated by blockchains are not only utilizable for native digital assets, but also for any type of asset which can be tokenized. However, blockchains allow for more than this as well. By taking a closer look at their architecture, one can realize that a blockchain network is comprised of a number of nodes that are able to send to each other both value and information, while constantly sharing and updating such record of transactions. This results in a powerful tool for coordinating communities, hierarchies or any sort of organization. In other words, blockchains can function as governance mechanisms. In recent years, this potential has materialized through the creation of decentralized autonomous organizations (DAOs) (Chohan, 2017). The governance properties of blockchains become more clear if analyzed through the lenses of institutional economics, which studies the different governance structures society has built to coordinate the exchange of goods and services, as will be further explained in the following chapters.

However, since blockchains have introduced an incredible amount of innovations from a technical standpoint, the intuitive first approach adopted so far has been to see it as a new 'Information and Computation Technology' (ICT) (Chuen, 2015). Many companies have realised that the security and transparency of blockchains allow for lower transaction, monitoring and auditing costs. As a result, in fields like supply chain and banking services, firms are beginning to adopt blockchain as a technology to increase the efficiency of their internal processes. The outcome that this technology-based approach suggests is that companies that will be able to develop and adapt quicker will have a competitive advantage over slower adapting firms.

Despite technology based approach being the dominant viewpoint as of today, there is an alternative perspective one can take in order to better understand the true socio-economic implications of blockchains. As introduced above, institutional economics and its focus on transaction costs, offer a governance based view which allows one to understand that blockchains are much more than a simple technology that will boost the next wave of innovations. In institutional economics, institutions are defined as coordination mechanisms for human interaction and exchange. These are: firms, markets, clubs and commons. Given their distributed and immutable characteristics, blockchains are also able to coordinate people and communities. Therefore, blockchain can be categorized as an institutional technology, or better, a technology for building institutions. In fact, blockchains in many cases turn out to be more efficient and secure coordination mechanisms when compared to the institutions listed above. Hence, there is a case for blockchains both complementing and directly competing with existing institutions (MacDonald et al., 2016).

In the past couple of years a number of new ventures have been attempting to exploit the governance based edge introduced by blockchains in the financial sector. This new field that leverages decentralized technology and governance for financial services goes under the name of 'decentralized finance' (Buterin et al., 2014, Chen and Bellavitis, 2020). One of its aims is to deliver the same or better services than the traditional financial system, while replacing centralized hierarchical governance with decentralized governance structures (Casey et al., 2018). Currently, decentralized finance applications range from decentralized exchanges (Bulat, 2018), to decentralized lending markets (MakerDAO, 2018) and decentralized financial derivatives contracting (Hashed, 2020).

The following research will utilize institutional economics theories to better understand the governance mechanisms of a number of blockchain financial applications, and will develop as follows. Chapter 2 will argument on how institutional economics theories apply to blockchain technology. In particular, the works of Coase (1937) and Williamson (1979) will be extensively discussed. This chapter will then present the research objective and relative questions. Chapter 3 will focus on the specific blockchain application that will be analyzed, decentralized exchanges, and how they reduce transaction costs when compared to traditional exchanges. Chapter 4 will present the methodology utilized to performs the analysis. Being it a multi-case study, the case selection rationale is presented along with data acquisition methodologies. Chapter 5 analyzes the projects selected by means of the Institutional Analysis and Development framework developed by Ostrom (2010) and finally draws the results. Chapter 6 concludes and recommends future work.

2

Research Outline

The following chapter will first utilize the theories of Coase (1937) and Williamson (1985) to argue that blockchain is an institutional technology given its ability to reduce certain type of transaction costs. Next, blockchain applications in the field of finance and their current governance mechanisms will be discussed. From here a knowledge gap is identified in the lack of consistency when approaching the study of these governance mechanisms. Finally, the chapter concludes with a formulation of the research objective and questions.

2.1. Blockchain as institutional technology

To better comprehend blockchains and their disruptive potential, from both technical and economic perspectives, it is necessary to first understand how society has evolved in coordinating exchange. From a high level standpoint, blockchains are known to allow for transaction cost reduction, therefore rendering value chains more efficient. At the time of writing this approach and narrative are dominant. Clear examples are the partnership between IBM and shipping giant Maersk to optimise cargo transport and relative information flow (Lal and Johnson, 2018), and the development from governments and central banks of Central Bank Digital Currencies (CBDC) for efficient monetary policy implementations, among other scopes (Ozili, 2022). Intuitively, new technologies are adopted when they create productive efficiency gains. However, when trying to understand how blockchains effectively reduce transaction costs, one can actually comprehend that they can also enable new coordination mechanisms. Or in other words, new institutional forms, as defined by Coase (1937) and Williamson (1979).

In the first half of the past century, the British economist - and later Nobel laureate - Ronald Coase, was the first one to theorize that transaction costs are one of the main drivers of the structure of the economy. Transaction costs are the costs related to: (i) searching a counterparty for the trade (e.g. buyer or seller), (ii) negotiating the terms of the exchange, (iii) verifying that goods or services being exchanged correspond to the ones established in the terms and (iv) making sure that the terms of the exchange are met correctly (enforcement). With his studies, Coase (1960) set the foundations for the field of studies of new institutional economics (NIE), also known as transaction cost economics, where institutions are defined as the social and legal rules that coordinate exchange. In other words, institutions are coordination mechanisms. In particular, in his groundbreaking essay 'The nature of the firm', Coase (1937) questions why would some exchanges take place under certain institutional arrangements as corporate hierarchies (firms) rather than markets. He concludes that because of transaction costs relative to uncertainty, asset specificity and frequency of dealings, such exchanges are more efficient if conducted in the former rather than the latter.

The key insights to be drawn here are that transaction costs not only determine the relative efficiency of institutions, but they can also be regarded as the costs for coordinating economic activity. Therefore, as blockchain reduces transaction costs and allows for new ways of coordinating economic activity, it can be defined as an institutional technology.

Behavioural assumptions

The new theories introduced by Coase did offer an explanation on the relevance of transaction costs in coordinating economic activity and in particular why and how hierarchies could be more efficient than markets (Coase, 1937). However, Coase did not clarify the exact conditions and circumstances under which a transition from one institutional regime to the other would occur. This task was carried by the American economist Oliver Williamson nearly half a century later in a series of academic articles (Williamson, 1985). One of the very first distinctions made by Williamson was between short-lived exchanges - also known as 'retail sales' - where the execution of the contract and payment occur simultaneously, and exchanges where the realization of both ends is time asynchronous. In other words, when there is economic relationship. The former depicts spot markets exchanges, as the ones one incurs in retail shops. The latter refers to exchanges as employment contracts and supply contracts. These are long term contracts where the exchanges between the two parties (e.g. labour and salary) occur at different times. From Williamson's perspective, contracts that execute over time and therefore require an economic relationship between the two parties, are characterised by a different set of risks, hence costs (Williamson, 1981).

In long term contracts, the core distinction made by Williamson (1985) was between *ex ante* and *ex post* costs, as displayed in Figure 2.1. *Ex ante* costs are the costs incurred before signing the contract, being costs related to negotiation, agreement safeguarding and contract drafting. On the other hand, *ex post* costs are the costs of enforcing the contract. Williamson (1985) identifies the problem when the terms of the contract set a priori diverge from their actual realization. These are defined as 'maladaptation' costs which consequently alter *ex post* costs as contract enforcement needs to be revised. For instance, this is true for cases where natural disasters impede the delivery of goods or services which have already been paid for. This forces the two parties to set up dispute resolution mechanisms and re-enter negotiations as well as secure the agreement once again. Therefore, *ex ante* and *ex post* costs are closely interdependent and both have to be carefully accounted for in early stages of negotiations in order for exchanges to execute as smoothly as possible.

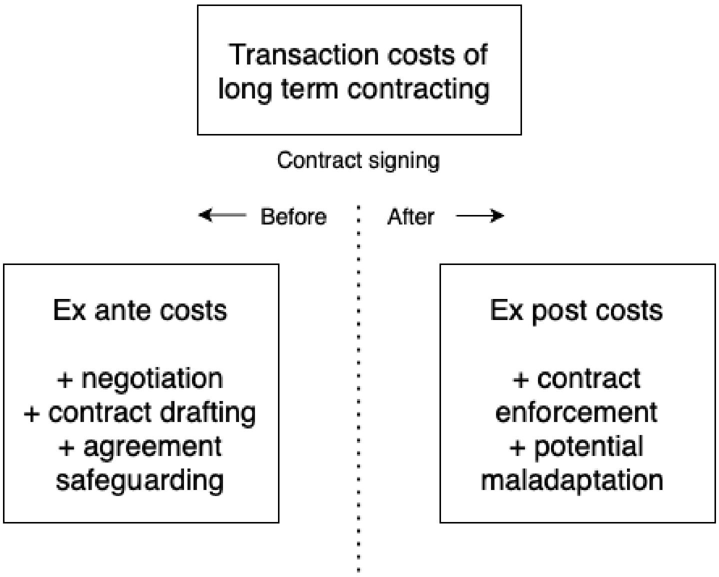

Figure 2.1: Ex ante and ex post costs of long term contracting (Adapted from Williamson (1996))

As explained above, contracting is a non trivial process which can be subject to flaws and can lead to other agreement difficulties. In the attempt to further understand the nature and key drivers of contracting, Williamson (1979) emphasized two major behavioural characteristics - common to every human being - that in his view influence the contracting process the most: bounded rationality and opportunism. Bounded rationality is the understanding and acceptance that the human intellect is limited. In particular, Williamson discusses two different dimensions in which rationality is to be considered bounded. The first one is the actual limit to the amount of information the brain is capable of acquiring and processing. Drawing a parallelism with computers, our rationality has a limited computational power. The second manifestation of this characteristic is in our inability to fully translate into words the precise nature and meaning of our thoughts. The result of this being that many of the contracts written are incomplete and do not account for all type of contingencies.

The second behavioural assumption presented by Williamson is the one of opportunism, which he defines as 'self seeking with guile' (Williamson, 1979). Meaning, not only are individuals self interested, but they also aim at their selfish objectives in deceitful and cunning fashion. In this view, moral hazard and adverse selection are two expressions of opportunism deriving from information asymmetry between contracting parties. However, Williamson believed that opportunism is more than just an effect of selfish behaviour and that is also comprises 'the incomplete or distorted disclosure of information, especially to calculated efforts to mislead, distort, disguise, obfuscate, or otherwise confuse' (Williamson, 1985). In that very same article, Williamson realizes that his definition of opportunism 'has turned out to be a controversial formulation' raising critics and concerns. Nonetheless, one could argue that the high degrees of opportunism and moral hazard that led to the global financial crisis (GFC) in 2008 more than validate and underline his point of view.

Finally, on top of the two behavioural assumptions outlined above, Williamson (1979) introduces the concept of asset specificity. In contrast with mainstream economic theories, Williamson recognizes that assets are far from being homogeneous in terms of the inherent costs of transacting them. As such he identifies four different types of specificity: site specificity, physical asset specificity, human capital specificity and dedicated specificity.

Contracting processes

In Williamson's view, the three constraints of bounded rationality, opportunism and asset specificity ultimately dictate the choices made by individuals when it comes to contracting. Table 2.1 below displays the type of contracting process deriving from the absence of one of these constrains respectively.

Asset specificity	**Bounded rationality**	**Opportunism**	**Contracting process**
Absent	✓	✓	Short-tem (markets)
✓	Absent	✓	Planning
✓	✓	Absent	Promise
✓	✓	✓	Hierarchy (firms, governments)

Table 2.1: Contracting processes deriving from absence or presence of bounded rationality, opportunism and asset specificity (adapted from Williamson (1985))

In the absence of asset specificity and presence of both bounded rationality and opportunism, contracting will be defined as short term. In other words, the process of exchanging goods is short lived as in typical retail shops. Therefore, the absence of asset specificity is what characterizes exchanges that take place in markets (Williamson, 1985). In the case where the only absent constraint is bounded rationality, the contracting process would simplify as the trading parties would be able to write extensive contract agreements covering every possible contingency, namely planning. This would also imply no possibility for maladaptation costs to arise, as every possible ex post outcome would have been foreseen and accounted for ex ante.

On the other hand, the absence of opportunism in any given exchange would allow for a highly efficient and straightforward contracting process, as none of the involved parties would have to worry about the other one being unfair (Williamson, 1981). In this particular case it would be enough for the trading parties to promise to make each other whole in any unforeseen circumstance. Even if maladaptation costs would arise given some sort of externality, it would be very simple for parties to renegotiate as none of them would act opportunistically given the high degree of trust.

Unfortunately, both opportunism and bounded rationality are inherent to human condition, therefore planning and promising are two extremely rare contracting processes. Finally, we are left with the case where all of the three constraints are present. For Williamson (1985), when asset specificity is introduced alongside bounded rationality and opportunism, the contracting processes migrates from markets to hierarchical organizations because the latter turn to be more efficient in dealing with specific assets than markets. Hierarchies can therefore be defined as organizations that protect users from the consequences of opportunism and bounded rationality while dealing with asset specificity.

From the discussion above one can already infer how the presence of trust can facilitate and economize the contracting process. To put it differently, trust costs are the costs which are incurred while attempting to mitigate against opportunistic behaviour (Williamson, 1985). As a result, the higher the trust, the lower the trust costs. This is also one of the main reasons why institutions exist, to provide a layer of trust where participants feel safe exchanging. Everyone trusts their local supermarket that products will be of a certain quality and not expired. In the same way, people trust their banks to keep their funds safe and to facilitate money transfers or withdrawals when required.

Blockchain and ex-post opportunism

As a result of the discussion above - given that bounded rationality and opportunism are inherent in any exchange - planning and promise are rare and hardly viable contracting processes. Hence, markets and hierarchies are the two dominant institutional arrangements society has adopted for coordinating exchange. However, Williamson (1996) did realize that promise would be a feasible form of contracting if the two (or more) parties involved were able to trust each other more. This would potentially be the case if contracts were self enforcing, therefore also reducing significantly ex post opportunism. Self enforcing agreements are exactly one of the major innovations introduced by blockchains through the utilization of 'smart contracts'. The concept and definition of a smart contract was first introduced by computer scientist Nick Szabo in the mid 1990s. He explains that it is a 'computerized transaction protocol that executes the terms of a contract' (Szabo, 1997). Moreover, Szabo foresaw that self executing contracts would not only reduce the need for trusted intermediaries but would also reduce transaction costs related to fraud loss, arbitration and enforcement costs.

This being said, in order to truly understand how blockchain technology effectively reduces transaction costs by minimising ex post opportunism (enforcement costs), one should analyse closer the argument developed by Williamson (1985) about costs and control of opportunism.

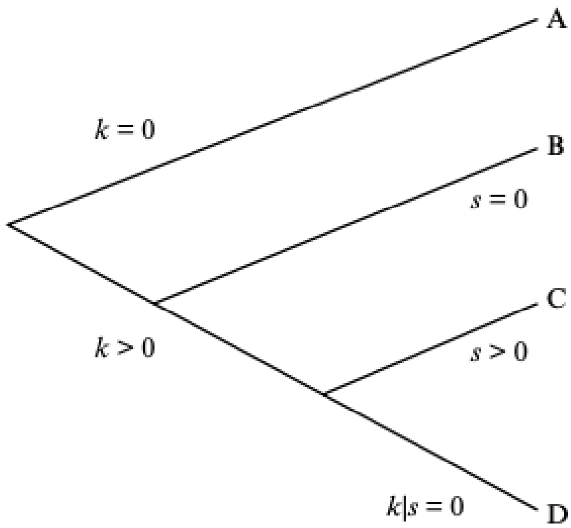

Figure 2.2: Cost and control of opportunism (Williamson, 1985)

In Figure 2.2, k represents the risk of opportunistic behaviour associated with asset specificity. In the absence of opportunism, k equals zero. On the other hand, s represents the safeguards put in place to protect from opportunism (k). Both of these parameters translate into costs endured by the parties during contracting phase. In the case were asset specificity is not present, then $k = 0$. Absence of opportunism implies that no safeguards are needed, hence also $s = 0$. As discussed in the previous section, this leads to short term market exchanges and in Figure 2.2 it is represented by instance A.

However, in the presence of asset specific opportunism, at least one of the two parties will want to protect themselves by utilising safeguards. For instance, this could be the case of someone wanting to buy a second hand product directly from another person rather than a normal marketplace. In this particular example, the buyer has no guarantee that what he is being sold matches exactly what he is being told to be sold. He is solely trusting the selling party. Being there no safeguards means $s = 0$. Having both the risk of opportunism and no protection against it means that the transaction could be subject to manipulation. In other words, information asymmetry is likely to occur, at the expense of one of the two contracting parties. Therefore, either the transaction may not occur at all - as one of the two contracting parties does not want to bear the risk - or it could occur at a loss for either the buyer or the seller. This is represented by instance B.

Nonetheless, in order to overcome the risk of opportunism, today a wide range of safeguards are available. For instance, in the example above of second hand buying, nowadays there are reputation systems that help the buyer in assessing whether a particular seller can be trustworthy or not. Furthermore, reputation systems also incentivize sellers to well behave as the better their reputation, the higher the chances they have to sell their products (Hendrikx et al., 2015). Theoretically speaking, safeguards as just explained should be enough to overcome the risk of opportunism. However, it is worth mentioning that in modern day institutional arrangements the cost of implementing safeguards is carried by the parties involved in a transaction. On one hand, buyers incur the costs of searching and verifying the right product. While on the other, sellers incur the costs of building their own reputation (Lui and Ngo, 2004). This means that, by adding the costs of opportunism and costs of safeguards (k + s), there are a number of exchanges that could never take place as their potential marginal gains is offset by the costs of k + s. In other words, where the costs of opportunism and safeguard implementation are too high, then a number of exchanges are not economically viable. Instance C in Figure 2.2 represents this case.

The discussion above provides one of the best possible angles to understand blockchain's disruptive potential. So far, society has developed in a way that safeguards are built in order to protect from opportunism, and the cost of both is carried by the contracting parties (Williamson, 1996). Blockchains completely revolutionize this as self executing smart contracts eliminate ex post opportunism, while the cost of validating and executing the contract is carried not by buyers and sellers but by network validators, namely miners (Calvão, 2019). This implies that $k|s = 0$ and is represented by instance D. That is, given the presence of safeguards, the cost of (ex post) opportunism is null. The reduction of opportunism costs k and the delegation of safeguards costs s, means that transacting on blockchains becomes more efficient and secure than modes B and C described earlier. Validators are the ones responsible for the security and integrity of the network bearing the cost of safeguarding through energy consumption. Moreover, they are economically incentivized to validate transactions as they receive transactions fees. It becomes now clear how transacting on blockchains is more efficient than in existing institutions.

The argument of trust

The power of self executing smart contracts lies in their ability to automatically enforce terms and conditions without the risk of these being altered by any of the transacting parties (Zheng et al., 2020). If one were to imagine himself as being either the buyer or the seller, one would realize that not having to worry about contract enforcement, whether it means payment or delivery of services, allows for a smoother negotiations and economic relationships. If suppliers had the absolute certainty that every client would pay for the supplied products and in established time, then economic activity would increase in number and efficiency.

Following this logic is how one can understand the concept of trust being a feature of blockchains (Berg et al., 2019). In the example just presented, buyers and sellers do not get to trust each other more, but they do trust the smart contract to deliver payments and supplies in due time and under the predefined conditions. To put it differently, contracting parties would now shift their trust from the institutions responsible for contract enforcement, to code that executes regardless. Existing institutions are composed by individuals which are themselves subject to opportunism. Moreover, resolving opportunism comes at a cost. On the other hand, code is non corruptible and enforcement costs are carried by validators.

This line of thought allows one to truly grasp what Williamson (1979) meant when he argued that trust is not an antonym for opportunism but actually a solution for it. As a matter of fact, empirical evidence has proven that the role of trust is central in overcoming social dilemmas (Rothstein, 2005). By being able to trust an automated contract, the risk of (ex post) opportunism gets annihilated. As a result, transactions that today occur under corporate hierarchies are now more efficient and viable on blockchains. 'Trust is the belief or assurance that another party will not exploit our vulnerabilities', this the definition of trust provided by Williamson (1979). Markets and hierarchies have evolved over time to provide a trust layer for exchange coordination. This layer of trust, as explained above, comes at a cost to users themselves. Furthermore, trust costs are the costs incurred while mitigating against the risk that a counterparty will be dishonest and act opportunistically. Blockchains have the ability to change this as they provide both an economic and technical solution to the problem of trust. In other words, blockchains offer a new solution for providing trust while reducing the costs of providing it. Therefore, some academics have also labeled it as a new technology of trust (Capece et al., 2020).

The utilization of smart contracts and immutable ledgers have the potential to disrupt existing mechanisms of exchange coordination. Nonetheless, smart contracts can be utilized for much more than just autonomous execution of economic contracts. As a matter of fact, utilizing these protocols as actual digital contracts is merely one of the multiple possible applications. Smart contracts are de facto being also utilized for imposing sets of rules and coordinating the behaviour of digital communities (Chohan, 2017), therefore enabling what are also defined as decentralized autonomous organizations (DAOs), effectively new institutional forms and subject of interest of the following section.

2.2. Problem statement

As discussed above, blockchains are much more than an ingenious technological innovation capable of disrupting existing Information and Communication systems. Given their technical architecture, blockchains are also powerful mechanisms for coordinating communities. In academic terminology, blockchains are an institutional technology of decentralization. As a matter of fact, the dualism to underline here is that blockchains can be utilized to create ecosystems in need of governance (decentralized applications) while at the same time providing the means to govern them (Allen et al., 2021).

One of the particular aspects of blockchains is that given their technical flexibility and characteristics they can be programmed to either replicate existing governance mechanisms - as hierarchies or commons - on a decentralized digital realm, or to create entirely new rules for coordination (Berg et al., 2019). The technical attributes that can be tuned and modified to establish coordination rules, thus institutions, are: consensus algorithm utilized (being the mechanisms according to which every node of the network agrees simultaneously on the state of the network itself), transaction capabilities (being the number of transaction the network can handle in a given amount of time), fees and rewarding systems (being the game theory behind incentive schemes for validators), security, privacy and codebase (Tasca and Tessone, 2017).

Berg et al. (2019) present blockchains' complementary and competitive institutional nature visually in Table 2.2 below. As one can see, before the invention of blockchains, dated 2009, governance mechanisms were firms, governments, clubs, commons and markets, with the first two being the only two to be hierarchically organized. After 2009, blockchains present the opportunity to function both as complementary governance mechanisms or as an entirely new one.

Before 2009						
Hierarchically governed						
Firms	Governments	Clubs	Commons	Markets		
After 2009						
Hierarchically governed						
Firms	Governments	Blockchains	Clubs	Commons	Blockchains	Markets

Table 2.2: Economic institutions of capitalism (adapted from (Berg et al., 2019))

As Berg et al. (2019) put it, blockchains are a 'generic governance mechanism: what we call a 'universal Turing institution". The definition comes from a parallelism with the definition of Turing machines (computers), which states that if a problem is computable at all, then it is computable on a Turing machine (McBride, 2015). Then a universal Turing machines, is a machine able to replicate the work of any other Turing machine. Therefore, a Universal Turing institution, is an institution which can replicate the characteristics and properties of any other governance mechanism. Nonetheless, even if theoretically all of the aforementioned is true, and blockchains can potentially enable entirely new institutional regimes, for the time being governance mechanisms currently being built and utilized by blockchain applications mostly resemble existing institutions rather than exploring new ways of coordinating (Allen et al., 2021).

Before addressing the governance models currently being implemented it might be useful to provide some historical context for clarity. As presented above, blockchain itself as a technology, first appeared in 2009 with Bitcoin (Bitcoin being the blockchian network and bitcoin being the digital asset exchanged on the network) (Nakamoto, 2009). The Bitcoin blockchain has a single and simple task which is to send and receive bitcoins in secure peer to peer fashion. Bitcoin was blockchain's sole application until 2015 when Vitalik Buterin co-founded a general purpose blockchain, Ethereum, in order for anyone to develop decentralized applications (Buterin, 2014c). Over the past six to seven years, the space has grown and matured and a number of ventures have tried to build applications as decentralized social networks and decentralized market places. However, all of these application are in their very early stages of development and none has yet achieved mainstream adoption (Schär, 2021). Of the different applications, one of the few sectors that have arguably grown considerably in user base - and only in the past two years - is the one relative to financial services, in particular lending markets and exchanges (Schueffel, 2021).

Blockchain and financial applications

According to the different contracting processes and their relative transaction cost characteristics argumented above, one can recognize financial intermediaries as one of the best positioned industries to embrace both technical and institutional upcoming innovations. Banks have existed for centuries and among their main functions has always been to safely store and manage liquid capital, precious metals and other financial products (Cetorelli and Peristiani, 2012). These are assets subject to the three characteristics discussed by Williamson (1996). The elements of both bounded rationality and opportunism are always present, while at the same time they possess the features of physical and dedicated specificity. Given these combinations, corporate hierarchies (banks) have been always the most efficient coordination mechanism for their exchange.

However, over the centuries financial intermediaries have evolved to more than just storing and managing assets. By pooling the excess amount of capital deposited by savers, banks are also able to create lending markets when and where there is excess demand for capital. This makes of banks, internal capital markets (Ben-David et al., 2017). By doing this, banks effectively intermediate entities willing to lend their capital in excess with entities that are willing to borrow it. Borrowing and lending is therefore a financial service which has been, thus far, only viable thanks to financial intermediaries.

In addition to borrowing and lending, financial intermediaries have also developed venues, known as financial product exchanges, for investors to buy and sell securities as bonds and equities. Participants rely on intermediaries as exchanges for various purposes as: safekeeping their financial products, efficiently finding a counterparty in case a security wants to be bought or sold, and finally clearing and enforcing the exchange of assets (Lees, 2012). In institutional terms, if a participant wishes to buy a security, the costs of finding a seller (searching), writing the contract (negotiating), monitoring the exchange (verification) and enforcing the terms (enforcing) would make it prohibitively expensive for the buyer to participate. As a result, hierarchies structures as firms have developed as the most efficient institution for coordinating these type of exchanges.

Other than storing assets and facilitating the matching between borrowers and lenders, and buyers and sellers of securities, there is a third key function that banks perform, the management and operation of payment rails. Banks keep records of transactions in their centralized ledger, whether these transactions are of payments or balances updates between multiple parties (Bushman, 2016). Not only banks intermediate between entities also thanks to their centralized bookkeeping, but when capital has to move from one account or bank to the other, banks also provide the means for doing so, as the Single Euro Payment Area (SEPA) in Europe (Schaefer, 2008).

Given the various services that financial intermediaries provide and discussed above, it becomes clear how blockchains have the potential to disrupt this industry. Fundamentally speaking, blockchains are a distributed and immutable registrar of secured transactions (Di Pierro, 2017). A transparent and immutable ledger is significantly more secure, trustworthy and less corruptible than a centralized non transparent ledger managed and monitored exclusively by a hierarchical organization prone to opportunism and moral hazard. This means blockchains have an edge from both monitoring and verification perspectives. As a result from this, the task of matching buyer and sellers, borrowers and lenders, would also become increasingly more efficient on a blockchian. Furthermore, blockchains also compete directly with payment rails as SEPA and, also in this case, have the potential to optimize transaction costs. Transacting on blockchains (sending and receiving assets) can be faster, more secure, permissionless and, most notably, does not require the approval nor monitoring from any third party (Di Pierro, 2017).

As a result, in the same way financial intermediaries as hierarchies exist given their comparative economic efficiency compared to markets, blockchains are developing to disrupt the economic logic and efficiency of intermediaries, as they prove to be more efficient in both intermediation and payment rails provision. Decentralized finance, or DeFi, is the name of the branch of applications in the blockchain space that is currently building the infrastructure for financial intermediation on blockchains (Schueffel, 2021). As it currently stands, the two applications that have had major growth in terms of both adoption and technical development are decentralized exchanges and decentralized lending markets. Nonetheless, other sectors are also growing as insurance protocols and derivative markets (Jensen et al., 2021).

The following research will focus on the specific application of financial product exchanges. Later chapters will describe in dept how this new technology is able drive down the costs of transacting financial products compared to traditional exchanges as the New York Stock Exchange (NYSE). In conclusion, as argued by Williamson (1985), transaction costs are the main drivers for institutional regimes. Therefore, having blockchains reduce transaction costs for financial exchanges, one would expect a governance shift in accordance. The following section will elaborate on the governance models that are currently being utilized for governing decentralized exchanges.

(De)Centralized Governance

To better understand how the governance of decentralized finance (DeFi) projects compare to public companies it may be useful to draw some parallels. Broadly speaking, public companies have two levels of governance, the board of directors and the management. The former, is responsible for identifying the strategy, overseeing the management and is usually composed by a number of directors and shareholders. The latter is responsible for the execution of daily operations within the company. Organizational structures built on blockchains work differently. Shareholders are replaced by token holders which can effectively participate in the decision making process of the project. On the other hand, the protocol (code) substitutes the management completely. This of course increases operations efficiency by placing 'automation at the center and humans at the edges' (Buterin, 2014b).

One of the principal promises of blockchain was to take advantage of its transparency and immutability not only for value exchange (digitally native and tokenized assets), but also for organizational coordination. This is possible through the implementation of Decentralized Autonomous Organizations (Buterin, 2014b). First launched in 2016 with 'The DAO' by the Ethereum foundation, DAOs would lever the key features of blockchains to render collective decision making secure, reliable and decentralized. From a governance perspective this represented a radical change as decision making would not only transition from being in the hands of a centralized management to virtually the entire user base, but moreover, the whole process of proposing, voting and implementing a new rule or feature would be totally transparent. As some researchers have defined it, blockchain would bring a higher degree of democracy, at least in theory (Merkle, 2016).

In practice, decentralized governance is currently resembling more traditional forms of governance, at least in this early stage (Davidson, 2021). At the time of writing, there are three major governance approaches in the blockchain space. Founder controlled being the first one. This means that the founder, which usually is a core developer, is the sole responsible for all the decisions concerning the strategy, the roadmap and its implementation. For early stage projects this is not necessarily a bad characteristic as it ensures a faster and more agile organizational regime. On the other hand, it also puts majority of the power in the hands of who actually cares and is responsible for successful progress. The second governance model is council control. This model gives control mostly to a group of core developers and investors which are considered to have the appropriate knowledge and tools to stir the project in the right direction. Such model has been successful so far for leading cryptocurrencies as Bitcoin and Ethereum, but does not provide the decentralization blockchains promise. Nonetheless, it presents similar advantages and disadvantages when compared to founder controlled projects, as decision making centralization and early speed of execution.

Finally, the third and most common model is a reproduction of representative or liquid democracy. Projects achieve this by distributing to all the users of the network so called 'governance tokens' (Froewis et al., 2021).

By being in possession of a governance token, a user is entitled to governance rights (residual control rights) and can either vote, or delegate their vote, on issues inherent to the project as: passing improvement proposals, modifications to the codebase or funding allocations. As one can infer, of the three governance mechanisms just described only the last one is an attempt to a different form of governance. Nevertheless, distribution of residual control rights through governance tokens comes also with its own degree of complexity and is further examined in following chapters.

Finally, what remains is that the space is still far from developing a new form of governance and current attempts are still in an early trial and error phase. While on one hand it is true that new type of institutions can be created with decentralized technologies, on the other innovative and decentralized governance models are currently non existent as blockchain applications are at best trying to emulate existing coordination mechanism, as for instance corporate governance (Allen and Berg, 2020). Founder and council controlled are clearly centralized decision making mechanisms no different from the ones utilized today by any startup. Decision making through governance tokens also comes with its own set of risks and difficulties as will be further explained in following chapters. For the time being, transaction cost reduction has not yet resulted in a fundamentally different institutional regime.

2.3. Knowledge gap

As a result from the discussion above, blockchain applications are yet to truly develop from an institutional perspective. That is, on how to govern both the protocol and the community. This presents an opportunity for studying and better analyzing existing decentralized governance models as to improve their design and resultant functionalities.

Thus far the coordination mechanisms that have been utilized by decentralized digital communities include informal polls, on-chain voting (meaning casting and registering each vote on the blockchain itself for transparency and accountability), online forums and formal improvement processes which are usually led by core developers or key additional contributors. Moreover, given that blockchains enable institutional versatility at a very low cost (Allen, 2019), the trial and error process by which governance mechanisms are designed and then tested has become faster over time. Perfect examples of such institutional tests include: (i) conviction voting, which gives users the possibility to continuously assert their preferred proposals instead of simply voting in a time boxed session, in this way the longer their support for a given proposal the higher the weight (conviction) of their 'vote' (Emmett, 2019); (ii) commitment voting, which is a variation of the previous system that also includes the amount of tokens a user has (Berg et al., 2020); and finally (iii) quadratic voting, which considers the intensity of a voters preference by allowing him to cast more than a single vote with the cost of each vote increasing quadratically with respect to the number of votes cast (Wright Jr, 2019).

Until this moment in time, all of these mechanisms and the resultant communities they have shaped have been analyzed by comparison with other governance mechanisms. For instance, distributing voting rights through governance tokens on a one token one vote basis has been compared to some extent to different forms of democracy (Allen et al., 2019). Nonetheless, concentration of voting power given concentration of governance tokens in the hand of a few owners is more a form of plutocracy rather than democracy (Buterin, 2018). Other projects have based their governance design on the assumption that blockchains could be governed as commons (intended as institutional form), therefore they have utilized to a large extent the design principles developed by (Ostrom, 1990), specifically designed for managing common pool resources. Finally, as discussed in the previous section, most of the nascent projects are experimenting with different forms of corporate governance (Allen and Berg, 2020).

While analysing and designing blockchain governance by analogy to existing and well known forms of governance has been useful to some extent, such categorization can be limiting as the industry matures and new coordination mechanisms arise. Designing a blockchain through a comparison with, for instance, a corporation, implies that one is emulating existing systems while at the same time disregarding possible innovation. Blockchain in itself is not easily and solely categorized as a club, firm, common or nation state. Therefore, an institutional agnostic framework of analysis might be a better approach to at least try to understand what are the new institutional possibilities. In this way, by analysing governance with an unbiased institutional perspective one may better understand its possibilities and pitfalls. Moreover, it would provide a currently lacking standardized and consistent method of analysis and design for the governance of blockchain applications. So far, no academic research has been conducted in this direction (Allen et al., 2021).

2.4. Research objective

As a result from the discussion above, the objective of the following research is to develop a better understanding of the governance mechanisms currently being utilized by the specific blockchain application of decentralized exchanges. Nonetheless, in order to gain such understanding the following research will utilize an institutionally neutral method of analysis such to obtain an unbiased perspective as well as to avoid the limiting institutional categorizations discussed in the previous section. For this reason the lifelong studies and work conducted by Ostrom (2010) in the past century on the governance of complex economic systems - which granted her a Nobel Prize in economics in 2009 - are of incredible relevance for the purpose of this research. In the late 1950s Ostrom found herself in a very similar position to where institutional economists focused on blockchain stand today. At the time, Ostrom was trying to find a way to challenge the market-government dichotomy which was dominant in that period. The market-government dichotomy stated that markets were the optimal institution for the production and exchange of private goods, while governments were the go to institutions for coordinating, imposing and enforcing rules against the exploitation of public goods as security and peace (Hobbes, 1904).

After decades of research, Ostrom (1990) was able to demonstrate empirically that in some circumstances hierarchical organizations as governments were not the most efficient way to coordinate groups of people around the utilization of public goods with a certain degree of rivalry, that is common pool resources. As a matter of fact, she discovered that these type of common resources as forests and fisheries were often better managed by the community itself, or commons. A great example was the expedition to Nepal to compare government and farmer managed irrigation systems (Lam et al., 1998). After a long on field research, they discovered that irrigation systems that were managed by the farmers themselves performed better in (i) the physical condition of the irrigation system, (ii) the amount of water available for farmers at the tail o the system during different season and (iii) the agricultural output of the system. Among the reasons for this higher performance was that farmers did communicate between them informally on a regular basis, they were able to develop their own agreements based on their own needs, they could establish monitoring systems and sanction for the community members that did not respect the rules. As a result, they were able to produce for yield and manage a fair and equitable system.

In her attempt to better understand these communities and a wider set of coordination mechanisms, Ostrom eventually developed a general and flexible framework for the analysis of any sort of institutional setting, namely the Institutional Analysis and Development framework (Ostrom, 2010). The IAD framework was designed to comprehend a general set of building blocks which could be utilized by analysts to categorize diverse coordination mechanisms. As Ostrom (2005) described it, the IAD 'provides a meta-theoretical language to enable scholars to discuss a particular theory or to compare theories'. As a result, since the IAD framework was conceived to holistically analyze unexplored governance structures with the goal of understanding their core functioning mechanisms, it makes sense to utilize this very same approach for studying the new governance structures introduced by blockchain, and in regards to decentralized exchange applications in particular.

Research question

So far the exchange of financial products has been coordinated by hierarchical organizations namely, firms (Petram et al., 2011). This because, given the relatively high transaction costs associated with the exchange of such products, hierarchical forms of governance have resulted in the most efficient coordination mechanism developed by society for these types of goods (Williamson, 1985). Coase (1960) theorized how in fact, transaction costs determine on one side the boundaries of the firm, and on the other the extent of their vertical integration. That is, when transaction costs are high, it becomes cheaper and more efficient to bundle transactions and functions together in firms rather than markets and contracts. On the contrary, when transaction costs decrease, vertically integrated firms should unbundle given that markets and contracts become cheaper to utilize (Coase, 1937).

New institutional technologies as blockchains are allowing for these type of transactions to be coordinated by institutional regimes that differ from legacy ones. As a matter of fact, for the first time in history, the final arbiter in exchange coordination of financial products is not a group of hierarchically organized individuals but an open source and self enforcing hard coded set of rules that execute on a public and immutable record of transactions (Berg et al., 2019). When systems become more decentralized, markets are a more valuable way to communicate and coordinate, being markets regarded as decentralized systems that create and reveal decentralized private knowledge (Kiesling, 2019).

As the means of coordination change, and with them the costs of transacting, new possibilities for governing these type of exchanges arise (Allen, 2019). Currently, a number of new governance mechanisms are being tested (Froewis et al., 2021). However, the study of these very systems has been thus far categorizing and inconsistent (Allen et al., 2021). For this reason, the following research will utilize an institutionally agnostic method of analysis to have a holistic and true understanding of the institutional innovations brought by blockchains. Therefore, in line with the approach taken by Ostrom (2010) more than half a century ago.

In light of everything discussed above, the edge provided by institutional economics in the study of blockchains and their governance becomes more clear. In sum, on one side the reduction of transaction costs is a driver for shifting institutional regimes (Williamson, 1985). On the other, the Institutional Analysis and Development framework developed by Ostrom (2005) provides the means for a deeper understanding of such institutions. As a result, given that blockchain arguably reduces transaction costs for transactions related to financial products, the main research question the following research will answer is:

'What institutional innovations does blockchain technology introduce to the exchange of financial assets?'

In order to better address the research question, a number of sub research questions that follow logically from the main one were formulated. First, one must understand how do blockchains effectively reduce transaction costs associated with financial product exchanges from an institutional perspective, therefore better comprehending whether vertical integration unbundling effectively occurs. This introduces the question which will be answered in the next chapter:

SQ1: *'How do decentralized exchanges reduce transaction costs compared to traditional financial exchanges?'*

Furthermore, in the same way Ostrom (1990) collected empirical data on the communities who's governance she intended to analyze, data will have to be gathered in order to implement the IAD framework as intended for the communities around decentralized exchanges. However, while Ostrom's communities lived in physical locations she could visit, the communities that will be analyzed in the following research are exclusively digital. Meaning all of their interactions, from less formal to formal occur online and often in anonymous or pseudonymous fashion. Different data gathering techniques will therefore be needed. Such methodologies for retrieving and analyzing data will be tackled in chapter four and will answer to the second sub research question:

SQ2: *'How and what data can be retrieved for implementing the Institutional Analysis and Development framework?'*

Next, in order to assess the performance and characteristics of different governance mechanisms by means of the IAD framework, a set of evaluative criteria are to be defined in the context of the analysis (Ostrom, 2005). Therefore leading to the third sub research question:

SQ3: *'How are evaluative criteria defined and why?'*

Finally, based on the institutional insights drawn from the implementation of the IAD framework, the following research will try to answer whether the transaction cost reduction brought by blockchains, has yet effectively propelled an institutional change as theorized by Williamson (1996). As a result, the fourth and last sub research question to be answered will be:

SQ4: *'In virtue of Institutional Economics theories, has the reduction in transaction costs associated with financial exchanges actually modified their governance structure?'*

3

Financial product exchanges

The following chapter will focus on the particular financial application central to this work, exchanges. First, an explanation of how traditional exchanges work will be provided followed by an illustration of the life cycle of a trade and the main players in the process. Next, decentralized exchanges will be introduced, followed by the innovative exchange model they introduce and the impact it has on the trade life cycle. Finally, other key differences between traditional and decentralized exchanges are discussed.

3.1. Traditional (centralized) exchanges

In order to truly understand how blockchains are able to disrupt the transaction process of certain financial instruments it might be useful to explore how these transactions take place today and the different parties which are involved in it. In this regard, the following section will delve into capital market infrastructure and the life cycle of financial instruments from the moment a trade is ordered until the moment it is settled.

Before delving into the analysis it is useful to point out that the products being transacted on exchanges, as securities, are subject to the three characteristics defined by Williamson (1985) of: bounded rationality, opportunism and asset specificity. As a result, in line with the theory of Williamson (1979), these type of transactions are more efficient when coordinated by hierarchical structures (firms), operating under corporate governance. As a matter of fact, multiple firms performing different actions during the trade life cycle are necessary in order to trade financial products (Loader, 2019). The appellative of 'centralized exchanges' derives from the fact that all operations, as in matching buyers and sellers and settling transaction, are carried out by a central authority.

There are a number of different financial instruments which can be traded on traditional centralized exchanges. These vary from financial securities to national currencies to financial derivatives (Harris, 2003). Each of these products can utilize different types of market infrastructure based on the complexity of the product itself and the regulations that are imposed on them (Loader, 2019). For simplicity, the following section will cover - at a high level - the market infrastructure concerning securities. Securities can be grouped into two main categories: equity securities, and debt securities. A good example for the former are stocks, or company shares. Where stocks entitle its holders to a partial ownership of the company's equity and in some cases also provide a claim on dividend payments and voting rights. The latter refers to bonds, whether issued by corporations or governments. Bonds are issued by these entities in order to raise capital. On the other side, bond holders can be entitled to interest payments and will receive back their principal payment on a predetermined future date (Bali et al., 2009).

Another important aspect to mention is that on exchanges one can trade in both primary and secondary markets, where the distinction between the two is non trivial. The primary market refers to the initial sale of a given financial instrument. For instance, an initial public offering (IPO). Primary markets therefore, only concern the initial transaction between the issuer of the financial product and the initial investor. On the other hand, once the product is sold to early investors in the primary market, investors can then trade these assets between them in the secondary market (Harris, 2003). The main takeaway of the distinction between these two markets is to note that exchanges provide a multi purpose venue where companies and governments can both market their equity or debt, as well as a venue where investors, whether individuals or corporations, can trade these products among them.

With all this being said, one can now explore the various steps of the life cycle of a trade. As visible from Figure 3.1 below, the process is divided in two main parts: pre-trade and post-trade (Perucchini, 2017). As one can notice, exchanges play only an arguably small part in the process of exchanging financial instruments for cash and vice versa.

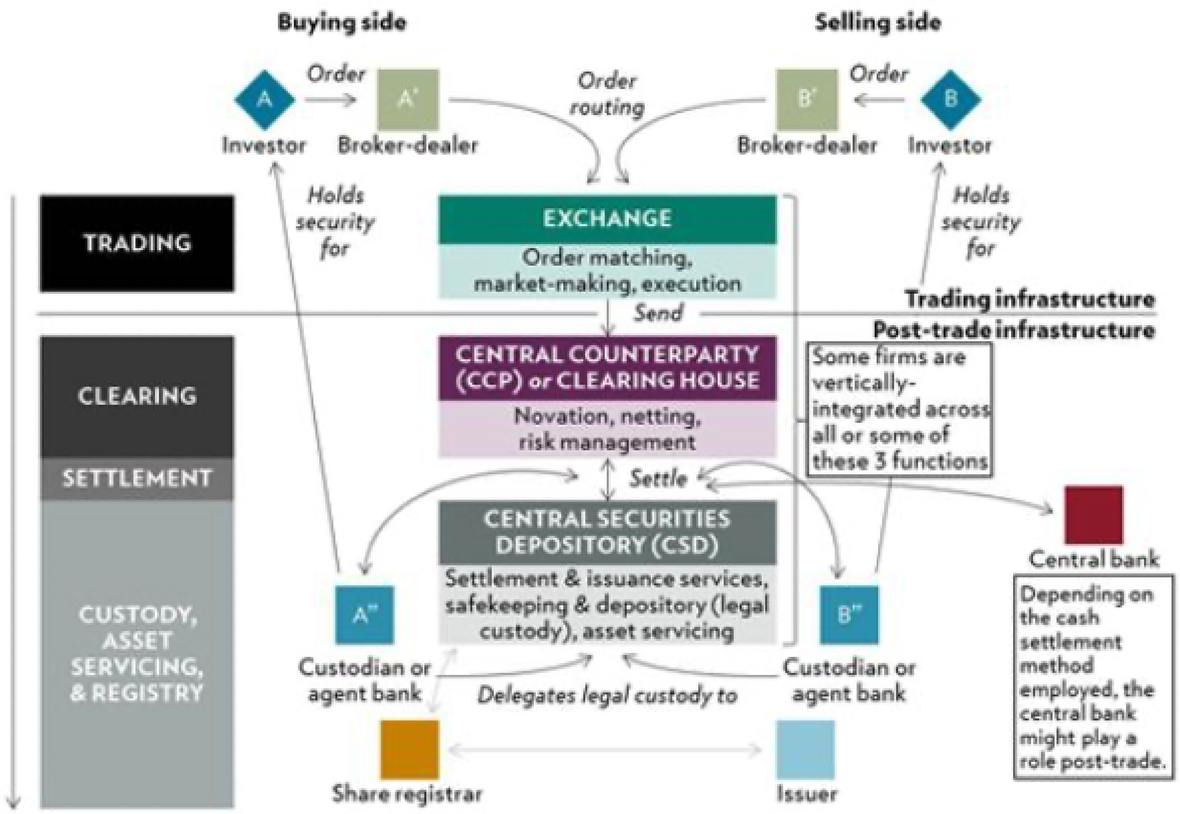

Figure 3.1: Pre-trade and post-trade market infrastructure (Perucchini, 2017)

Pre-trade

The pre-trade and trade segments of the transaction process for financial instruments consist of order submission, matching and execution. All of these three tasks occur on the exchange venue itself (Collomb and

Sok, 2016). As mentioned above, stock exchanges are market places where buyers and sellers interact to transact different financial products. Therefore, they must be able to market their own assets (order submission), find a counterparty willing to buy or sell to them their asset (order matching) and finally, execute the order once the two parties agree on transacting terms. However, the actual (physical) exchange of assets does not occur immediately nor on the exchange venue itself but at a later stage in the post-trade process (Loader, 2019).

Nowadays the entire process of submission, matching and execution occurs electronically and the biggest exchanges in the world in terms of amount of listed assets and volume traded are: the New York Stock Exchange (NYSE) in the US, Euronext (ENX) in Europe, the Tokyo Stock Exchange (TSE) in Japan and the Shanghai Stock Exchange (SSE) in mainland China (Lees, 2012). Exchanges developed in the early XVII century as physical venues where brokers could meet to trade assets as stocks and bonds. While the first ever stock exchange was established by the Dutch East India Company in Amsterdam in 1602 (Petram et al., 2011), today Wall street is the largest and most well known stock market place in the world.

Order books

In order to match buy and sell orders, exchanges utilize the so called order book model. Order books are electronic records of the buy and sell orders that traders submit to the trading venue (Puljiz et al., 2018). There are two different types of orders a trader can submit: market and limit orders. When a trader submits a market order he is indicating that he is willing to buy (or sell) the asset at the current market price. On the other hand, limit orders are used to indicate a price in which one is willing to either buy or sell. The former are also referred to as takers, given that they 'take' the current price. While the latter are also defined as makers, given that they 'make' (create) buy or sell orders (Puljiz et al., 2018). Figure 3.2 is a visual representation of an order book. Usually, exchanges charge different service fees for maker and taker orders, which can vary from basis points, (0.75%) to up to 4% depending on the broker and trading venue (Watch, 2021).

Price	Quantity	Total Quantity
11254.9	0.66676358	18.97374802
11254.4	0.66666365	18.30698444
11253.5	0.25080000	17.64032079
11253.4	1.65441200	17.38952079
11253.2	0.56547391	15.73510879
11253.1	0.40000000	15.16963488
11252.9	0.26741127	14.76963488
11251.9	6.65222361	14.50222361
11251.8	7.85000000	7.85000000
11250.5 USD		
11250.3	0.26741784	0.26741784
11250.2	0.66666906	0.93408690
11249.3	0.88889208	1.82297898
11248.6	1.77400000	3.59697898
11247.5	0.66250000	4.25947898
11247.2	0.88909868	5.14857766
11247.1	0.88909536	6.03767302
11246.7	0.03750000	6.07517302
11246.0	0.10300000	6.17817302

Figure 3.2: Order book display (Watch, 2021)

As visible, $11250.5 USD is the current market price. The green numbers below it are all the buy limit orders (bids) placed by traders and the relative quantity per price level, displayed in the middle column. In the same way, the red numbers above the current market price represent the sell limit order (asks) set by traders, with the relative quantity on the right (Watch, 2021). Order books convey a large amount of data which can turn useful for investors and traders during decision making. For instance, by simply observing the quantities set to be bought or sold at different price levels, one can determine which of these are more relevant. Another way to look at it is to consider bids as demand and asks as supply of the given financial product. As a result, when demand outweighs supply one knows it is easier for the price to increase rather than decrease.

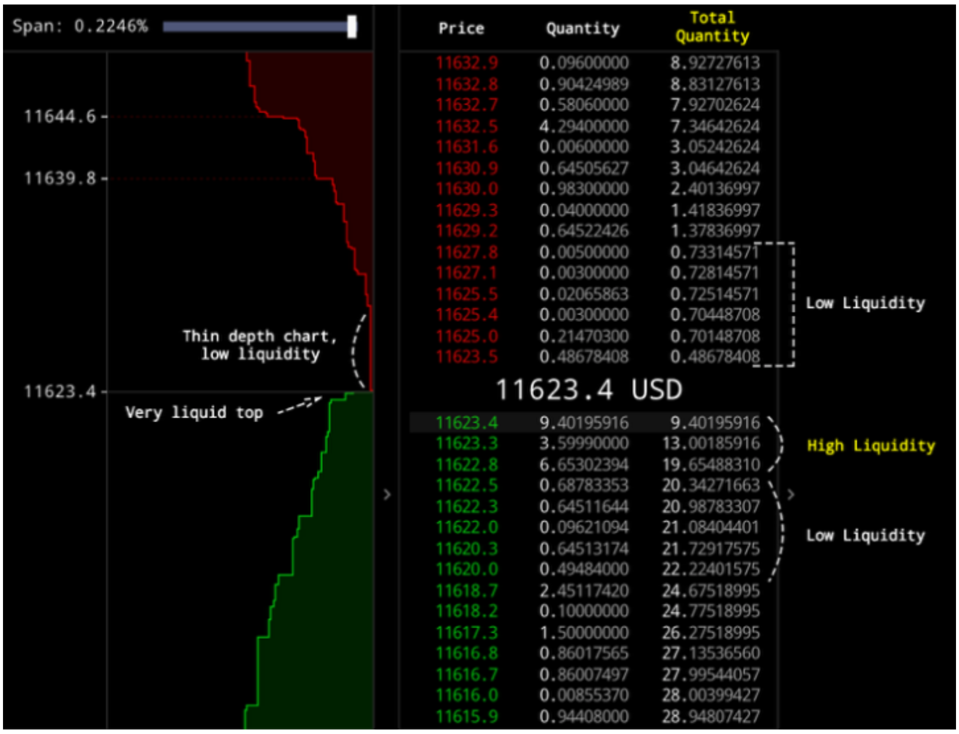

Figure 3.3: Market depth and liquidity visualization (Watch, 2021)

The data present in an order book can be also displayed as in Figure 3.3 above. Such display is called market depth. Market depth provides a more visually friendly representation of the cumulative orders per price level (Watch, 2021). One of the reasons why this tool can turn to be very useful is because it makes it straightforward to individuate the bid-ask spread. This is the difference between the lowest sell order (ask) and the highest buy order (bid). In other words, the difference between the lowest price a seller is willing to ask and the highest price a buyer is willing to pay. In markets with many participants and high transacting volumes, also known as liquid markets, usually the spreads are very low. On the contrary, in periods of low market volume and high uncertainty spreads can be large (Narayan et al., 2015).

Another important information provided by the market depth is the amount of liquidity present in the market at given price levels. The concept of liquidity is quite important as it indicates the ease with which a participant can convert his assets into cash and vice versa (Holden et al., 2014). For instance, if one is willing to sell X amount of assets at price Y, one must be sure that at price Y there are enough buy orders (bids) able to absorb the entire X amount. In case the amount of bids at price Y are cumulatively lower than X, then the matching engine of the order book will fill as much of X as possible at price Y, and sell the remaining of X at lower price levels. This would result in the seller selling at an average price lower that Y, the intended selling price. The amount of capital lost by selling the remaining amount of X at prices lower than Y, is also known as slippage (Holden et al., 2014). Or in other words, slippage is the difference between the amount X sold at price Y, and amount X sold at the average price smaller than Y. As a result, participants with large amounts of capital want to make sure they are trading in very liquid markets. Figure 3.3 shows visually how to find liquid price levels. Liquidity and slippage will be two important aspects considered when discussing decentralized exchanges.

Post-trade

After the orders are matched and buy and sell side agree on both quantity and price of the asset to be exchanged, the exchange executes the orders and notify traders on the successful transfer. However, the actual exchange of assets, for instance a security with cash, only occurs at a later stage and not on the exchange itself. The process from the electronic execution of the trade on the exchange until the final settlement of the trade is defined as post-trade process. The post-trade segment of the life cycle of a transaction has two major operational components: clearing and settlement (Loader, 2019).

Clearing

Clearing consists of all the necessary steps required to make sure that both parties involved in the transaction are effectively capable of meeting their trade obligations (Menkveld and Vuillemey, 2020). In other words, in a delivery versus payment trade (delivery of the asset and payment of cash), part of the clearing process is to address whether the buyer has sufficient funds for the purchase and the seller actually has the securities. For this information to be checked and controlled, the exchange submits to a clearing house all the necessary information of the trade and of both parties. Such information includes: price and quantity of the instrument, cash to be delivered, identifiers of the product exchanged, identifiers of the parties involved and their respective accounts (Amini et al., 2015).

One of the reasons why clearing is so important is to avoid trade failure due one of the parties missing their obligations (Amini et al., 2015). For instance, if an investor is willing to sell part of his securities to meet payment obligations elsewhere, incurring in a failed trade could mean not being able to deliver his other due payment. As a result, this could have a cascading effect on other trades and depending on how connected and tangled the market is this could have an epidemic effect. For this reason, for all the assets listed on traditional exchanges, clearing houses assume an additional role other than assessing the status of trading parties. For every trade executed on an exchange, the clearing house acts as Central Counter Party (CCP). In other words, the risk of trade failure is transferred from the trading counter parties to the CCP as the latter commits to guarantee both delivery and payment (Amini et al., 2015). As a result, the risk of trade failure is significantly reduced as even in the case of missed obligation from say, a buyer, the CCP will deliver the payment to the seller. The legal process by which the CCP can act as a counter party to both sides of the trade is defined as novation (Chamorro-Courtland, 2010). Figure 3.4 provides a better visual representation of the role of a CCP.

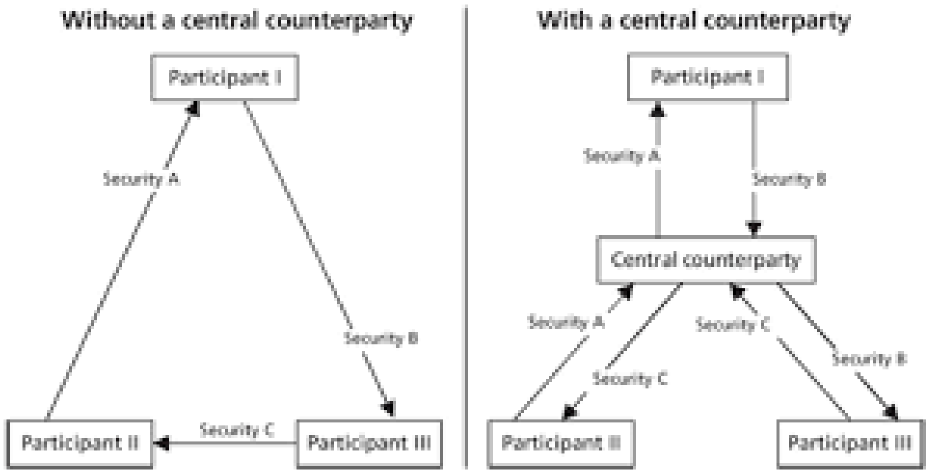

Figure 3.4: Central counter party visualization (Amini et al., 2015)

The revenue generated by the CCP derives from the fee it charges to exchanges for providing these services (Menkveld and Vuillemey, 2020). On top of this CCPs do not act as counter parties with their own capital and assets, instead they ask exchanges to post collateral which can be in the form of securities, capital or other financial assets. Based on the level of risk of the assets traded on the exchange, CCPs have different collateral requirements. Also, based on the volatility of the markets, collateral calculations and deposits can vary daily. Finally, an additional function conducted by clearing houses is the one of trade netting. Meaning, instead of clearing every trade, the CCP will calculate (net out) the position of every member at the end of the trading day and only clear netted trades to increase efficiency (Chamorro-Courtland, 2010). A practical example would be to consider Alice buying from BOB ten shares of a given stock in the morning and ten more in the afternoon. Instead of clearing two trades, the CCP will clear one single trade of twenty shares at the end of the day. This is of course an example with only two trading parties, CCPs are effectively able to net trades among several traders. This is called, multilateral netting, as showed in Figure 3.5. Moreover, the recording of all transactions from the CCP provide an additional and useful point for regulatory oversight (Floor, 2020).

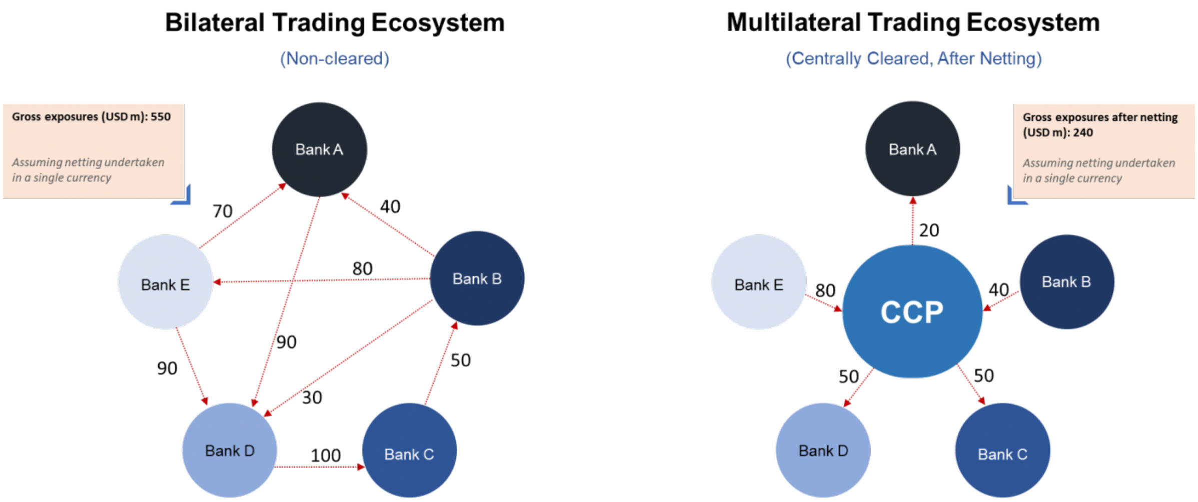

Figure 3.5: Netting process from a central counter party (Floor, 2020)

Settlement

After the clearing house dictates that both parties are able to meet their obligations, the settlement process starts. Settlement consists in the actual (physical) exchange of assets (Loader, 2019). Every trade has two different dates referring to it, first when the transaction was made, and second when the transaction was settled, or 'value date'. The latter is when the transaction actually happens. The format utilized to refer to these two days is written as: T+x. Where T is the transaction date and x is the number of days that pass between transaction submission and actual exchange. The vast majority of securities today are settled electronically and have settling times usually of two business days (T+2). On the other hand, government bonds are usually settled the next business day (T+1). Settlement times have improved considerably over the past few decades, in fact in the 1960s and 1970s settlements were done purely manually and exchanges closed on Wednesdays as settlements took more than 5 days (T+5). Transaction costs were as a result considerably higher.

There are two main players in the settlement process: the Central Securities Depository (CSD) and custodians. Custodians are entities that physically hold securities, in the form of certificates, for safekeeping. Usually, custodians are well known banks themselves. Today, the largest custodians in the world are, in order: BNY Mellon, State Street Corporation and JP Morgan, having nearly $68 trillion USD of assets under management combined[1]. Custodians custody securities the same way traditional banks custody capital for clients. The main difference is that while banks are allowed to invest that capital, custodians are not allowed in any way to financially allocate the assets they custody.

There are of course a wide number of custodians globally, each holding different securities and financial products. When two parties exchange assets held by the same custodian, for the latter it is easy to handle settlement as it only requires a simple book entry. In other words, settlements are handled internally. However, when trades occur where multiple custodians are involved and have to exchange assets between them, the CSD comes into play. A CSD can be seen as a custodian of custodians, covering a similar role to what central banks are for commercial banks when it comes to wholesale banking exchanges. While custodians can custody assets in multiple jurisdictions, CSDs exist at a national level. Meaning, each country has its own custodian of custodians with its own regulations. Just like every country has its own central bank. Therefore, CSDs are the ultimate responsibles for the settlement and safekeeping of securities. In addition, banks, custodians and exchanges are allowed to hold cash accounts with CSDs in order to facilitate the cash leg of transactions as well. In case no cash account in held with CSDs, the CSD will solely be responsible for the exchange of the security. While the transfer of cash will occur through a commercial or central bank.

CSDs also play a role in the issuance of new securities as the issuer must decide which CSD it wants to use for security registration. As a result, the CSD will also be responsible for checking that the amount of securities in circulations matches the amount of registered ones. CSDs also usually cover other asset servicing tasks as: tax reclaims, auditing of structured products and asset management. Nowadays, most paper certificates have been substituted by digital ones for efficiency increase in transacting it. This process is also known as security dematerialization. Figure 3.6 below provides an overview of the clearing houses utilized by the major European exchanges and the relative CSDs they utilize the custody their securities.

[1] Retrieved on 12/12/2021 on `https://www.institutionalinvestor.com/research/6565/The-World-s-Largest-Custodians`

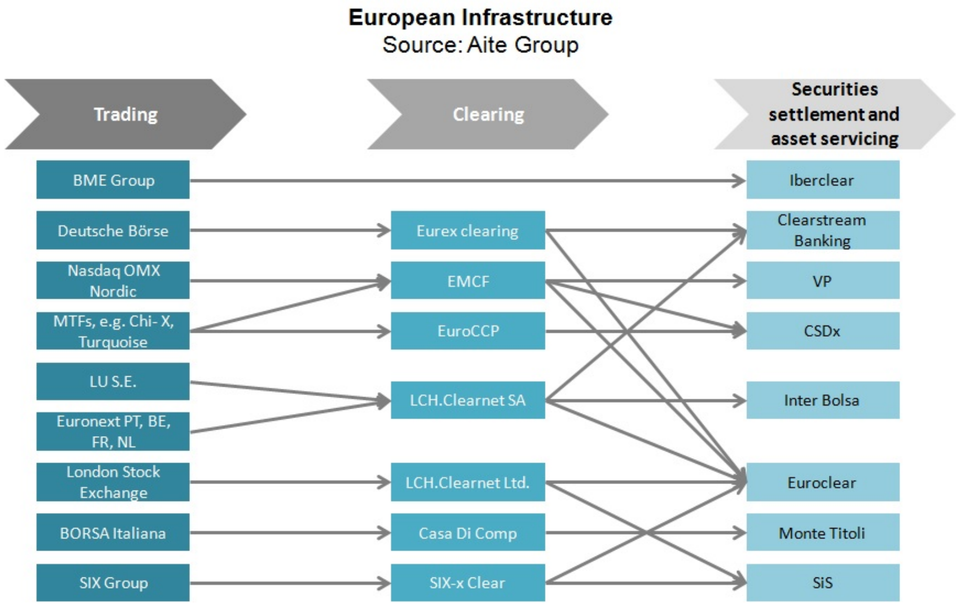

Figure 3.6: Main trading venues, clearing houses and central security depositories (O'Shea and Camerinelli, 2013)

Concerns with the current trade life cycle

As presented above, the current life cycle of a trade goes through several intermediaries and can take a couple of days in the best case scenario. While many intermediaries play a very important role for the security and accountability of the system, it does at the same time cost a significant amount of fees to end users. As a matter of fact, a study from (Wyman, 2015) estimates that the total amount of money spent in just clearing and settlement amounts to nearly $5 and $43 billion USD per year respectively. Other than the significant costs incurred there are other factors that are also negative and questionable about the current system. The scope of the following section is to both list and discuss such issues.

The first aspect to consider is the one of reconciliation. In finance, reconciliation is the process of comparing all databases and financial records in order to make sure they all present the same data regarding security ownership, account balances and other financial information. As discussed in the previous section, the transfer of ownership and cash between parties often goes through a number of different intermediaries as clearing houses, custodians and central security depositories. Each of these entities has its own registrar to track the movement and ownership of assets. Therefore, reconciliation is the process of synchronizing all the different registrars to present the same information. This task can become even more difficult as all these digital databases are often built using different digital architecture, thus rendering reconciliation more laborious. A research from (Aite, 2014) shows how only in 2014, the cumulative worldwide spending on reconciliation was estimated to exceed $1.07 billion US dollars.

The next risk to mention is the one of settlement time. As mentioned above, most trades today taking place on exchanges settle two business days after the trade date (T+2). Even though this time interval has significantly been reduced over time, it still exposes both counter parties (and the CCP) to a certain degree of risk. In fact, the value of the assets exchanged could drastically vary within a two day time span, or worse, one of the parties could default in the meantime. The collapse of huge financial intermediaries in 2008 during the Great

Financial Crisis are a good example of this sort of risk. Fortunately, blockchain technology today offers the possibility of instant settlement and clearing which will be discussed in the following chapter.

The last risk to be considered, which was already mentioned above is the one of failed trades. As mentioned earlier, these could translate in undesirable cascading effects. The reasons why a trade could fail are the following. First, settlement instructions could simply be submitted wrongly by one of the parties. Generally, these sort of errors tend to be resolved before settlement. However, when this is not the case the trade fails. The other reason is that either one of the two parties could lack the cash or security it was intended to trade. In these cases, the trade does not necessarily have to fail immediately. In some cases, trades could be partially settled including future total settlement when either the cash or the securities are readily available. Lack of cash or securities is the exact reason why CCPs perform their function, to take on insolvency risk. However, in case the CCP is not provided with enough collateral, it could go bankrupt as well. Nontheless, thus far only three CCPs have gone bankrupt (Menkveld and Vuillemey, 2020).

3.2. Decentralized exchanges

Given that blockchain is a technology that provides secure payment rails, asset tokenization, and a trusted shared record of information, it is not a big step to theorize how it could disrupt the currently cumbersome financial infrastructure for security exchanges. The following section will deep dive on how distributed ledger technology is currently attempting to improve both pre-trade and post trade processes through decentralized exchanges.

Automated market makers

For the pre-trade process, exchanges running on blockchain or, decentralized exchanges (DEX) are utilizing a model different from the order book model utilized by traditional exchanges. While the latter use order books to match orders from buyers and sellers, decentralized exchanges utilize a relatively new model defined as automated market makers (AMMS). AMMs where first theorized by Buterin (2017) (co-founder of Ethereum) and saw their first implementation with Uniswap in 2017 (Younessi, 2018). The scope of the following section is to broadly explain the functioning of AMMs as well as their relative risks.

As discussed in the previous chapter, one of the main challenges for exchanges is the one of guaranteeing enough liquidity for traders. In other words, guaranteeing there would be enough limit orders in order to avoid slippage and therefore have higher trading efficiency. AMMs tackle the liquidity challenge with the the use of liquidity pools. Liquidity pools are bundles of smart contracts that function as escrows containing, in most of the cases, a 50/50 balanced proportion of two different assets, where their relative price is a function of their proportional reserves within the pool. There are other models that contain different coin ratios. Nonetheless, the most popularized ones are the pools that split asset value amount equally (Liu and Xie, 2021). The following section will explain technically how the supply of the two asset in the pools are maintained stable.

Figure 3.7 provides a visual representation of how users interact with liquidity pools. For traders, or simply an individual that want to exchange one asset for the other, the process is straightforward. One deposits the asset one intends to sell on one side of the pool, and extracts the same value amount of the asset one is willing to buy from the other side of the pool. This is also known as swap. For every swap, traders also have to pay a fee. Different liquidity pools charge different fees. The main difference between this mechanisms and the one utilized by centralized exchanges is that, for every buy and sell order on an order book there must always be a counterparty willing to take the other side of the trade. On the contrary, on AMMs one trades against the other side of the pool and not other traders. While the former is a 'peer-to-peer' model intermediated by a centrally controlled matching engine, the latter is a 'peer-to-pool' or 'peer to contract' model running on a distributed network of validators.

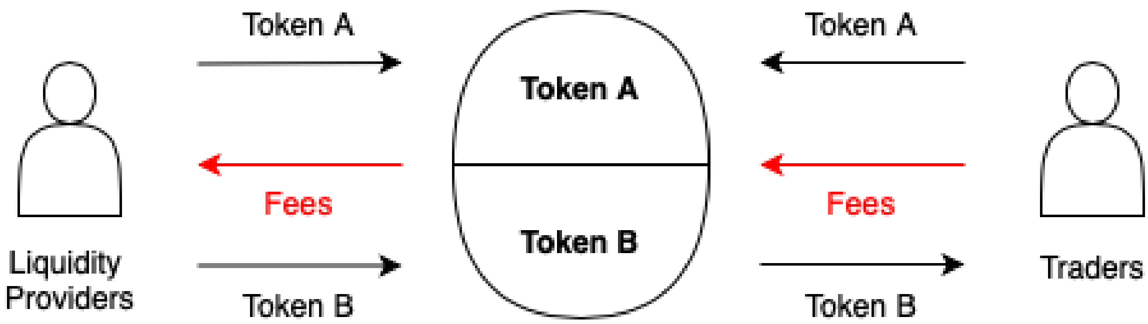

Figure 3.7: Automated market makers interaction visualization

In order book models, liquidity is provided by traders taking the other side of the trade. Given that AMMs function fundamentally different, traders and liquidity providers are two different categories of participants. Following the ethos of decentralization and permissionlessness, anyone with an internet connection and any amount of tokens can deposit liquidity in the pools. In other words anyone can be a liquidity provider. The only requirement is to deposit an equal $ amount of tokens on each side of the pool in order to keep it balanced. The incentive for depositing liquidity in the pools is that liquidity providers earn the fees that traders pay for swapping. Fee distribution is of course proportional to ones share of the pool. In other words, if there were only one individual providing liquidity in the pool, he would earn 100% of the fees generated. On the other hand, if there were three liquidity providers, providing respectively a total amount of 50$, 30$ and 20$, then the first one would be entitled to 50% of the total fees, the second one to 30% and the last one to 20%.

One can now start to grasp the game theory behind the usability of automated market makers. If one plans to be a liquidity provider, one would obviously look for the pool with the highest fees in order to earn more. However, traders on their side look to swap their coins on pools that have low fees. As a result, liquidity providers have to try to deposit capital in pools where the amount of swaps compensates for the low fees payed by traders.

Constant function market makers

One may now wonder how does the pool maintain a balanced amount of coins. After all, when a trader performs a swap, he is effectively increasing the amount of coins on one side and reducing the amount of coins on the other side. As a result, the relative price of the asset in excess trades at a discount, while the token in defect becomes more expensive compared to the other side of the pool. This creates an arbitrage opportunity for traders. Where arbitrage is the process of buying assets in markets where it trades at a discount and selling it in markets where it trades at a premium in order to capitalize on the difference. This means that automated market makers rely on arbitrageurs in order to make the price of the tokens in the pool converge with market price (Bartoletti et al., 2021). This being said, the two formulas that govern the balance of tokens within the pool are presented below:

$$P_a * X_a = P_b * X_b \tag{3.1}$$

$$X_a * X_b = k \tag{3.2}$$

Where, P_a is the price of token a, while X_a is the amount of tokens a in the pool, the same holds for token b on the right hand side of the equation. On the other hand Equation 3.2 is the 'constant product' or 'constant function' between token balance X_a and X_b. Their product k, must always remain constant (Wang, 2020). The main function of the constant product function is to ensure that the total value in the pool stays unchanged after each transaction. However, as explained above the relative amount of tokens per side does effectively change and arbitrageurs are incentivised to rebalance it. As visible in Figure 3.8 below, the amount of token in each side of the pool increase and decreases respectively when there are swaps. While providing liquidity (right hand side figure) means the the amount of assets on both sides will increase equally, as a result they product will also increase to a new value of k.

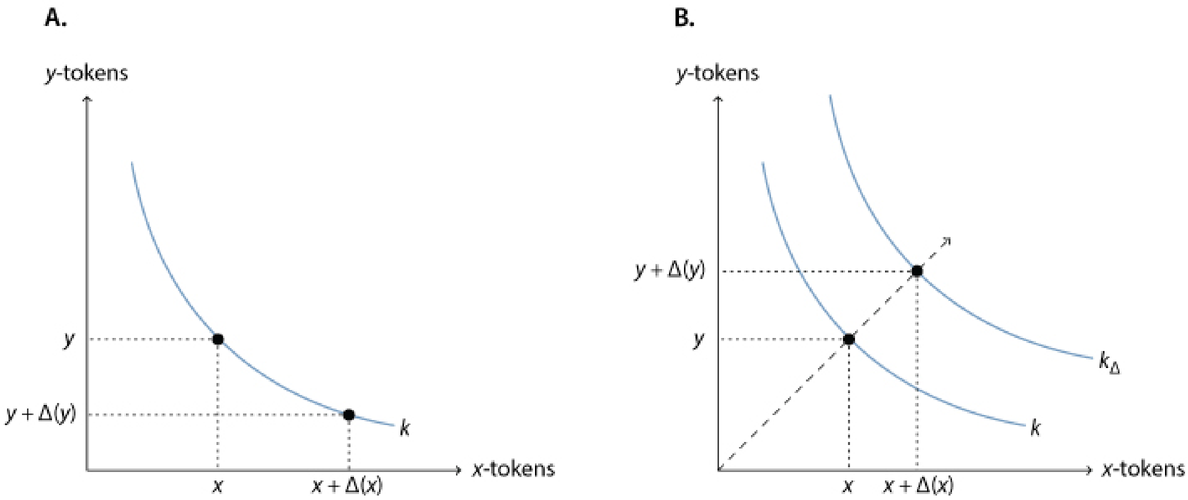

Figure 3.8: Constant function function market maker (Chitra et al., 2021)

Impermanent loss

One of the main risks to take into account when one intends to provide liquidity in a pool is the one of impermanent loss. That is, the loss of funds (risk) one is exposed to when depositing capital into liquidity pools (Jakub, 2020). Impermanent loss occurs given the relative change in price between the tokens in the pool. To better explain this type of risk exposure a practical example is provided below.

When one provides liquidity in a pool one is given in return a token representing ones share of the pool. This token, defined LP token, is the one utilized both to claim rewards accrued from fees and to withdraw the liquidity provided when desired. Let's suppose there is a pool containing ETH and USDC. USDC is a coin that has its value pegged to the US dollar, hence stablecoin. Now lets further assume that the price of ETH is $100 and the pool contains 10 ETH. As a result, one side of the pool will have 10 ETH worth $1000 in total, and the other side contains $1000 USDC. Assuming one had provided 1 ETH and 100 USDC to this pool, for a total value of $200, one had received an LP token worth 10% of the pool. In turn, this means that one is entitled to

10% of the total fees generated by the pool over time.

If the market price of ETH increases by 100% reaching $200 this would mean that the price of ETH in the pool would be trading at a discount compared to market price. As a result, arbitrageurs will take this opportunity to withdraw ETH from the pool and sell it elsewhere until the two sides of the pool are balanced. Eventually a new equilibrium will be reached when the pool contains 7.071 ETH (worth $1414.2) and 1414.21 USDC. If one were now to withdraw its 10% pool share, one would now have 0.7071 ETH (worth $141) and 141 USDC for a total of 282$. While 282$ is $82 above ones initial investment of $200, it is also $18 dollars below what one would have had by not providing any liquidity to the pool. That is, 1 ETH worth $200 plus $100 USDC. Therefore, the difference between, what one would have had by simply holding the tokens and ones new share of the pool is defined as 'impermanent loss'. The loss is labelled as impermanent given the fact that tokens can always return to their initial relative price, therefore granting liquidity providers their initial share distribution. Figure 3.9 below displays the impermanent loss experienced at different price variations. When a token increases 500% relative to the other, impermanent loss is around 25%. Meaning, 25% less in value with respect to what he would have had if he simple held.

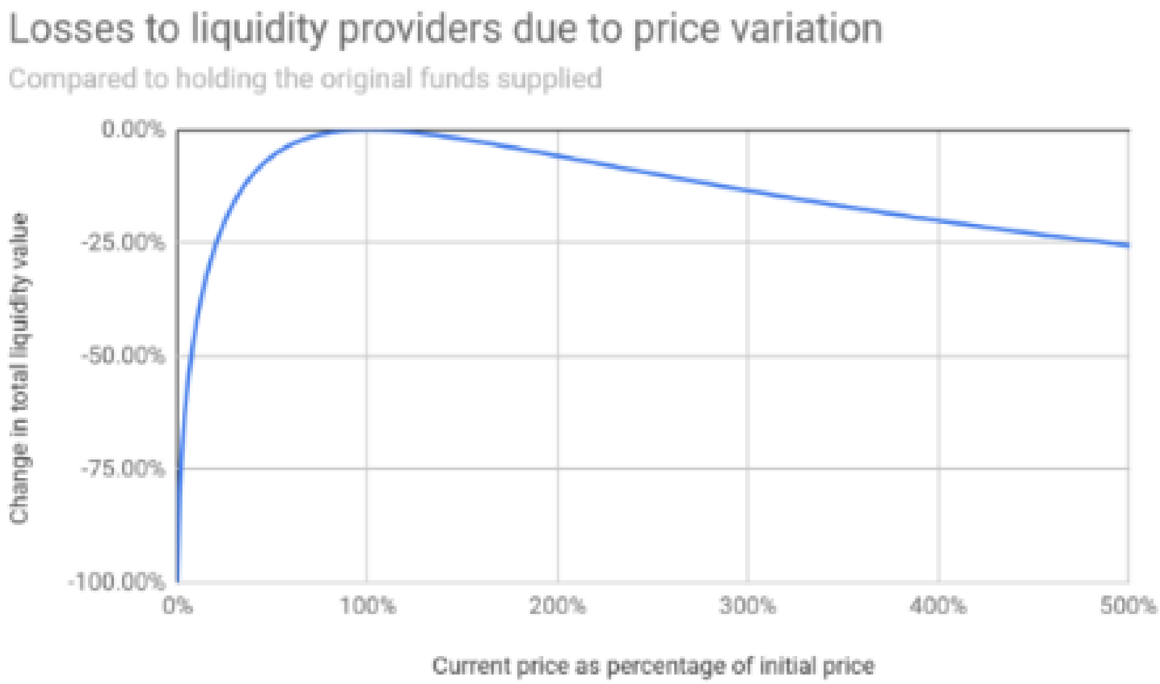

Figure 3.9: Impermanent loss based on different degrees of price divergence (Aigner and Dhaliwal, 2021)

A number of solutions for impermanent loss have been implemented over time. Some project, as Curve (better discussed in the following chapters), only provide pools of tokens that tend to have stable value relative to each other in time (Egorov, 2019b). In fact, the vast majority of Curve pools only hold pairs of stablecoins. This means that traders can only utilize those pools to exchange one dollar pegged asset for the other. Another more practical solution has been to change the ration of the assets held in the pool. That is, instead of having pool containing assets at a 50/50 ratio, other ratios as 80/20 and 95/5 have been implemented. A study conducted by Martinelli (2020) and visible in Figure 3.10 and displayed below shows in fact how impermanent loss reduces in pools with different ratios.

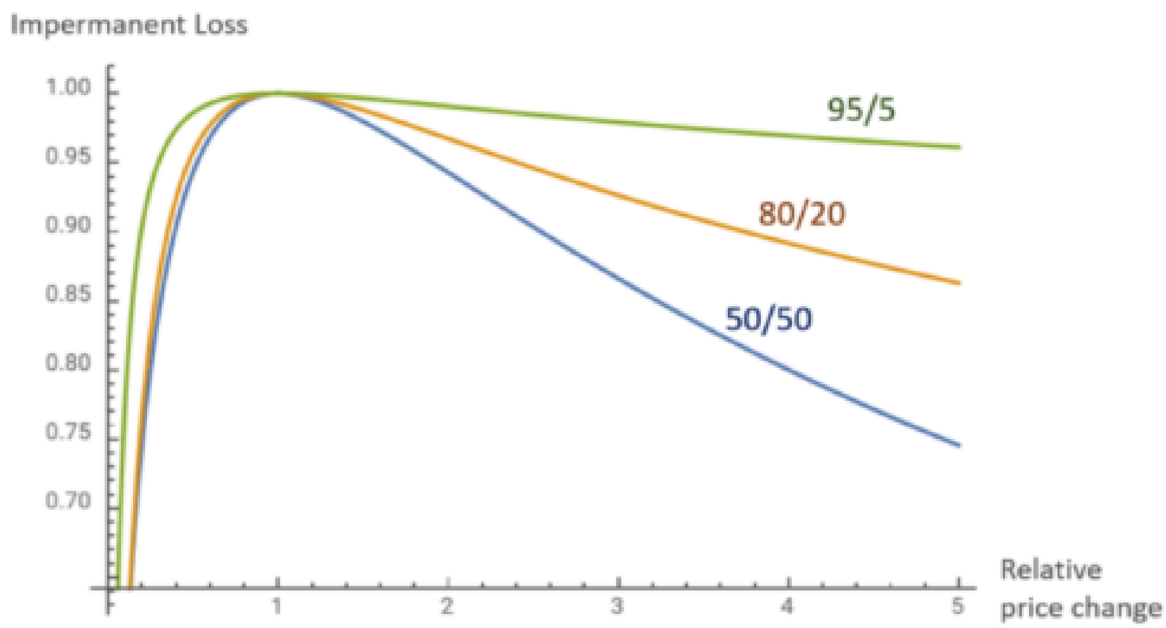

Figure 3.10: Impermanent loss based on different token proportions in the pool (Martinelli, 2020)

Another way of looking at impermanent loss is by studying Equation 3.1. Assuming the left hand side is a stablecoin and remains unchanged in both price and quantity, when P_b increases, X_b will have to decrease accordingly in order to maintain the same value of P_a * X_a on the left hand side. Furthermore, by substituting Equation 3.1 into Equation 3.2 and solving for X_b one would have Equation 3.3 below, that clearly shows how as the fraction P_a/P_b tends to zero, so does the balance X_b. Meaning the more the price of P_b grows relative to P_a, the less tokens X_b will be in the pool, and therefore in ones LP token.

$$X_b = k * \sqrt{P_a / P_b} \tag{3.3}$$

3.3. Differences between DEX and CEX

Post-trade disruption

The last section described how blockchains can impact the pre-trade process by substituting centrally controlled order books with decentralized automated market makers. Nonetheless, given the technical characteristics of blockchains, the post trade process is also prone to major disruption. This section will cover how current blockchains disrupt clearing and settlement, and provide an answer to the first sub research question *'How do decentralized exchanges reduce transaction costs compared to traditional financial exchanges?'*. Figure 3.11 provides a visual representation of this process.

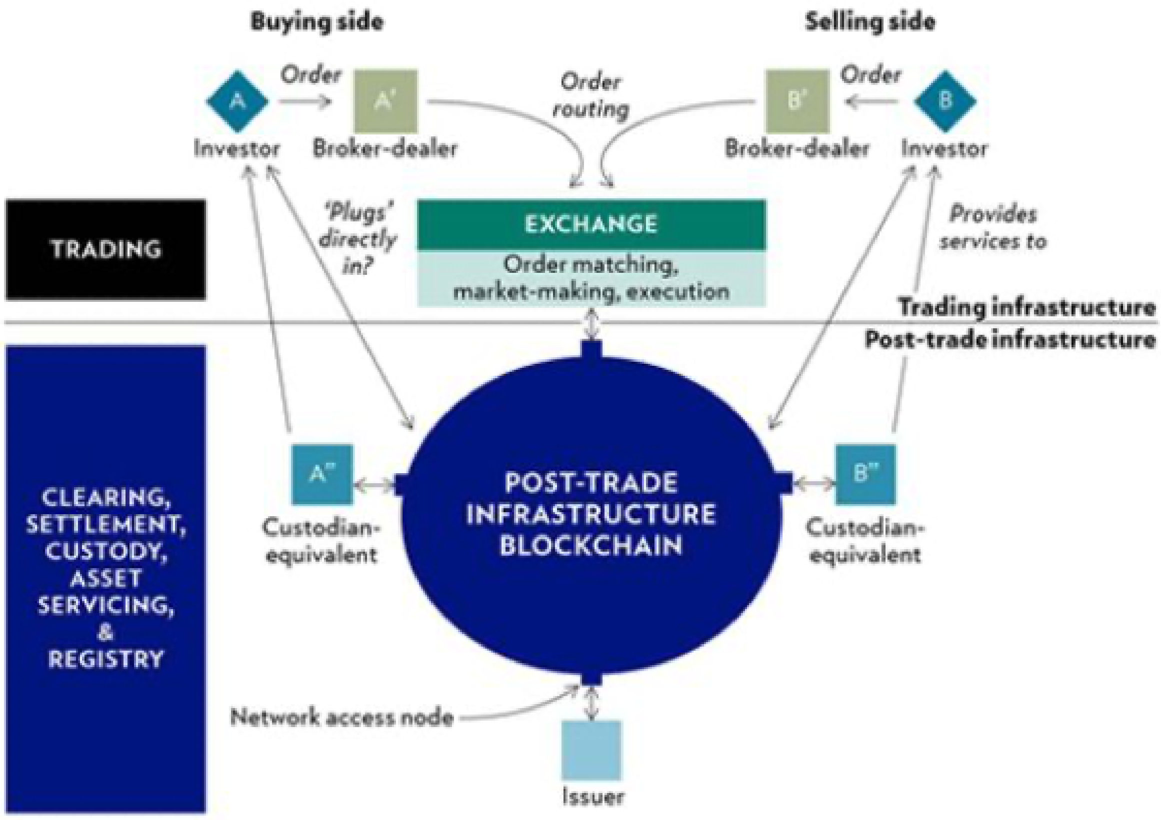

Figure 3.11: Blockchain disruption in post trade process (Perucchini, 2017)

As explained in the previous section, the clearing segment in post trade is the process by which the clearing house makes sure both parties are able to meet their trading obligations. However, clearing houses have developed to become more than this as well. The most important tasks they carry nowadays are: (i) taking the role of a central counter party (CCP) in order to take on the risk of default by one of the trading parties and therefore avoid failed trades; (ii) conducting multilateral netting in order to reduce the number of settlements and therefore improve efficiency; and (iii) finally, through multilateral netting increase collateral efficiency by reducing the amount of margin clients have to deposit to the clearing house. On top of this, the post trade process in the traditional financial sector is quite fragmented with some of the players overlapping in tasks, as for instance custodians and CSDs, and spending a big deal of time and money in database reconciliations.

Given that blockchains are shared and immutable records of information, they could be an incredibly valuable solution for post trade processes as they would quasi-eliminate the need for reconciliation. That is, everyone has already a synchronized database which is shared with all the other participants. Furthermore, by making settlements near instantaneously, as real time gross settlements (RTGS), many of these layers could be avoided and therefore reduce costs, time and risk. In addition, given that blockchains also provide alternative payment rails, they could be utilized not only as shared databases but also as a delivery versus payment (DvP) system. By then utilizing smart contracts, one could theoretically automize asset servicing as well, as tax payments and dividend claims.

Near real time settlements would also allow to save in capital requirements to be deposited on the central counter party, as the collateral needed for default provisions would decrease. Furthermore, counterparty risk would theoretically also decrease itself given that parties would be trading and settling directly between them. As a result, for clearing houses, the interests charged, liquidity risks and operations costs charged through fees would decrease substantially. In reality, near instantaneous settlements coupled with instant verification of cash balance and security holdings would theoretically render clearing houses redundant and could be disintermediated (Collomb and Sok, 2016).

As a result, the case for blockchain reducing transaction costs associated with the exchange of financial products is quite strong given that it impacts all of the stages of the trade life cycle. From disrupting the matching model, to the actual verification and exchange of products, to finally to provision of payment rails infrastructure for the transfer of goods.

Entry barriers

The fact that exchanges can now be executed with decentralized models does not necessarily mean they are better under every aspect, specially at the current state of development. The following section will outline all the major advantages and disadvantages of both centralized and decentralized models. For decentralized exchanges one of the main advantages is its permissionless nature. As stated earlier, this implies that virtually any person with an internet connection can use the service. From a compliance standpoint this has not proven to be too optimal, as lack of clear or consistent regulations have attracted a wide range of money laundering activities. However, for both privacy and accessibility decentralized exchanges are currently a superior solution. This goes in striking contrast with centralized exchanges where one has to first go through an account verification process and conform to the know you customer (KYC) rules. On top of this, one has to link his own personal bank account in order to send and receive funds. At the time of writing, around 1.7 billion individuals around the globe are currently unbanked[2].

Another advantage of decentralized exchanges is that there is no central authority controlling the system so there is no risk of opportunistic behaviour from exchange managers. Furthermore, in decentralized exchanges one never gives up the custody of his own asset until the moment the actual exchange is bound to happen. In centralized exchanges, for one to trade one must first transfer his own assets to the trading venue and then perform the trade. Thus, while one does not give up ownership on the asset, one does give up control. This as well, is subject to maladaptation risk from centralized exchanges. On the other hand, decentralized exchanges do currently face major difficulties. Even if the technology has experienced an exponential growth in the past year it still hasn't been able to attract as much capital as to make trading as smooth as it can be on centralized competitors. Therefore, liquidity, and therefore slippage, is still a major cause of concern, specially for large amounts of capital and during low volume hours. As for technicalities, decentralized exchanges have only recently provided the option for placing limit orders and margin trading, even though their implementation is still early. Other features though are still missing as the use of stop-losses. Nonetheless, the industry is in constant development and further innovations are planned to roll out in coming months and years.

Another major adoption blocker at the moment is with regards to fiat capital on ramp options. In other words, decentralized exchanges currently only function with assets deployed on a blockchain, whether digitally native or tokenized. This means that users still have to find a way to convert their national currency (fiat currency) into crypto-assets through some regulated entity. In order to do this, one does need a bank account. Therefore, this currently demystifies the notion that decentralized exchanges are accessible to everyone. As the market matures, solutions to this will mature as well. Furthermore, decentralized exchanges are currently

[2] Retrieved on 15/05/2021 `globalfindex.worldbank.org`

bounded to the transaction speed capabilities of the underlying blockchain (in this case Ethereum) which is currently limiting the scalability of these platforms. Last but certainly not least, the user experience and interface of decentralized exchanges is still far behind the ones of their centralized alternatives, Figure 3.12 presents the trading interface of the decentralized exchange Curve. This of course presents a great entry barrier for the less tech savvy individuals.

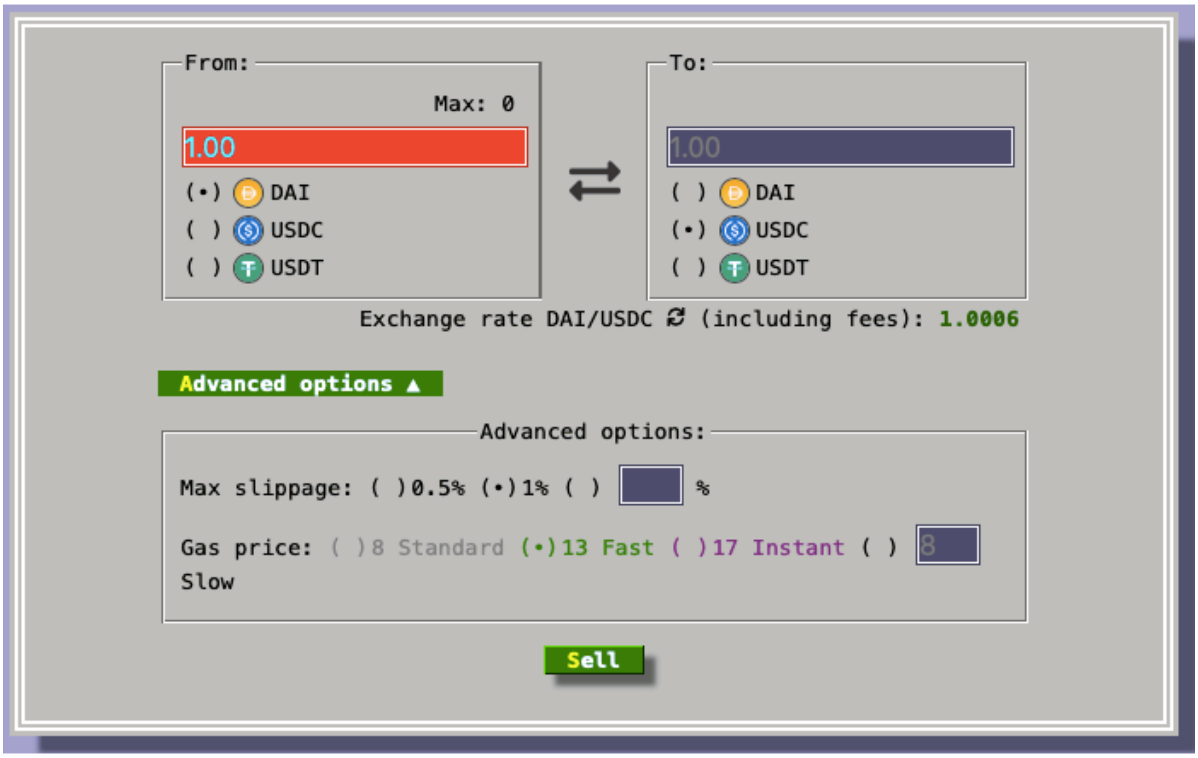

Figure 3.12: User interface of Curve decentralized exchange (source: `https://curve.fi`)

On the other hand, centralized exchanges have still a number of advantages over decentralized ones that keep them as a solution better preferred from majority of market, at least for the time being. Given their dominance and time in the market they do present themselves as more liquid solutions and therefore preferred by traders, particularly the larger and more active ones. They are also strictly regulated and have conform to consumer safety regulations that make participants feel more comfortable hence achieving their trust. Given their centralized nature, centralized exchanges have a higher performance when it comes to transactions per second. This is also a very relevant factor considered by users when deciding on which type of platform to trade. However, centralized exchanges also come with a set of disadvantages that make decentralized versions competitive. These are the opportunism and maladaptation risks one incurs when depositing capital into these platforms, the potential price manipulation from exchanges themselves and the entry barriers relative to account verification rules and the need for a bank account, as mentioned above. All of the different advantages and disadvantages of both centralized and decentralized exchanges are summarized for clarity in the Table 3.1.

	Decentralised exchanges	Centralised exchanges
Advantages	- Security (no third party intermediary) - Custody of assets - Permissionless (virtually anyone can exchange or create a market) - Privacy - Lower fees	- Better user interface - Regulatory certainty - Higher liquidity - Higher transaction throughput
Disadvantages	- Poor user interface and experience - Regulatory uncertainty - Less feature w.r.t. centralised competitors - Only support crypto assets - Lower liquidity - Scalability issues	- Not in control of funds - Permissioned (entry barriers) - Bank account required - Subject to maladaptation risks

Table 3.1: Centralized and decentralized exchanges, advantages and disadvantages

4
Methodology

The following chapter will first argue why the following research should follow a multi-case study methodology. Next, the rationale for the selection of the cases to be analyzed is outlined. The methodology for acquiring and analyzing data is then discussed in section 4.3. Finally, an overview of the IAD framework and its main components is provided in section 4.4.

4.1. Multi-case study methodology

For the following research the methodology picked to analyze and better understand governance models in the DeFi space is a multi-case study. Perhaps some of the strongest proponents of case studies research methodology are Yin et al. (2003), which states that 'case study research has a functional and legitimate role in doing evaluations'. Thus, as case studies can be utilized to understand the complexity of a case including both their temporal and contextual conditions. One of the main reasons for choosing this method is that there is not enough academic literature on the topic so most information has to be retrieved from the projects developing the project itself. This pragmatic approach also aims at supporting academics in developing their own fundamental understanding of this new technology and both its institutional and economic implications.

According to Walsham (1995), utilizing multiple case studies as a research methodology is particularly helpful is assessing 'why' and 'how' questions. While answering to 'why' can be sort of intuitive - to coordinate communities in better and more efficient fashion - answering to 'how' is a much more challenging task. Scrutinizing existing protocols and trying to understand 'how' they do it is arguably one of the best and most efficient research strategies at the moment. Moreover, Walsham (1995) also explains how theories developed from case studies built upon theoretical frameworks, like Ostrom's IAD framework, are generally helpful for the outcomes of an interpretative research. One of the risks of building on theoretical frameworks is to end up with narrow viewed analysis that risk to disregard a number of insights and further implications. For this reason, it is crucial to adopt an iterative process of data collection so to verify and validate the insights suggested by the framework application. Fortunately, as mentioned earlier, public blockchains supply any savvy researcher with copious amounts of data.

In support to what elaborated above, Ketokivi and Choi (2014) explain how 'theory elaboration' is a research case methodology where a general theory is utilized to approach the problem and subsequently, empirical data is utilized to validate or challenge the theory. The following research adopts institutional economics theories to frame the governance systems of certain decentralized financial applications, which are then further analyzed and elaborated with multi case studies.

Flyvbjerg (2006) highlights the importance of selecting a different range of cases in order to have a general and well informed overview. For this reason, the three projects chosen for the analysis diverge under a number of aspects as degree of adoption, growth trend, governance mechanisms and transparency from the core developers. The main source of data and information are the publicly provided documentations available on the projects platform, a number of well elaborated articles on the current state of development and data retrieved from blockchains explorers and analytics platforms. Moreover, all of these protocols have open discussion forums where participants can exchange opinions and proposals. Reading through these forums has been incredibly useful to understand the overall sentiment of the users and the real motives that push them to keep involved in the community. These forums are obviously much utilized by core teams as well as they can immediately receive feedback on new implementations or possible changes to the protocol.

4.2. Case selection rationale

As mentioned early in the report, the institutional analysis that will be conducted in the next chapters will focus on the particular application of decentralized exchanges. As of today, the two largest DeFi applications in terms of both capital and users attracted are (i) decentralized exchanges and (ii) decentralized lending markets. The former was chosen given the fact that it is actually the largest and most utilized among all applications. This also translates in more data and information available for the analysis. Considering the recency of these applications and the speculative rise they have experienced over the last couple of years, retrieving quality data is already a challenge in itself. Furthermore, finding and analysing projects that have the highest odds of perduring over time instead of simply being momentary fads also requires a certain rationale and probabilistic thinking. More than 200 different dexes are deployed on more than ten different blockchains. The following section will cover the rationale behind the final selection of three dexes.

The very first discriminant to utilize in order to reduce the set of eligible dexes is to consider only the ones that are native to the Ethereum blockchain. There are multiple reasons for this choice. First, Ethereum was the very first blockchain that could be utilized to deploy smart contracts - hence, applications - therefore it was also the first one where developers could start experimenting new protocols. In fact, all the first DeFi (and non DeFi) protocols where deployed on Ethereum. Figure 4.1 shows the total total value locked in dexes, per blockchain, since mid 2020. As noticeable, at the very beginning, Ethereum was the only blockchain where protocols where deployed. As soon as these protocols started to prove product market fit, other blockchains started to incentivize projects in order for them to deploy on their chains as well. As a result, today many dexes are deployed on at least 4 different chains. Figure 4.1 also shows how over time, other chains have grown considerably taking away market share from Ethereum gradually. However, for the time being Ethereum is still the most utilized chain. The second reason why it makes more sense to analyze dexes launched on Ethereum is because they are also the ones that have been for longer in the space. At most, protocols have had sufficient utilization for the past two year, this is a considerable lower amount of time compared to how long have traditional exchanges been in the market. 'Older' protocols also mean older communities and a core team that has been building in the space for longer. Therefore, it makes more sense to select among projects that have proven conviction rather than protocols that have perhaps only launched six months ago and have not yet proven technological nor community resilience.

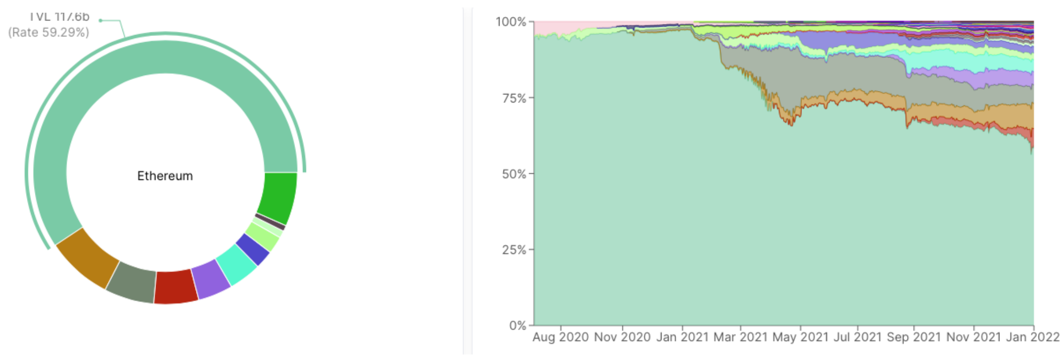

Figure 4.1: On the left: current Ethereum dominance by total value locked. On the right: Ethereum dominance since January 2020 in comparison to all other public and permissionless blockchains (source: `https://defillama.com`)

Now that protocols have been narrowed down to only the ones native to the Ethereum blockchain, the next factor to take into account is the amount of liquidity protocols have managed to attract. As explained in the previous chapter, the larger the liquidity on exchanges, the lower the slippage traders are subject to, and a result the smoother the functionality of the exchange. Again, given the earliness of these products, one may prefer to select the most developed ones as they hold a stronger product market fit. Liquidity can be measured by the cumulative amount of capital each decentralized exchange has locked in all its liquidity pools. This metric is also referred to as 'total value locked' (TVL). Figure 4.2 below displays the top 10 dexes on Ethereum by total value locked.

	Name	Chains	1d Change	7d Change	1m Change	TVL ↓
1	Curve (CRV)		+1.81%	-15.68%	-14.82%	$17.26b
2	Uniswap (UNI)		+2.35%	-19.93%	-27.20%	$6.15b
3	SushiSwap (SUSHI)	+4	+4.59%	-10.05%	-19.22%	$3.54b
4	Balancer (BAL)		+2.93%	-12.09%	-12.18%	$2.58b
5	Bancor (BNT)		+4.38%	-24.77%	-25.86%	$958.45m
6	Loopring (LRC)		+13.47%	-8.88%	-37.16%	$340.66m
7	ShibaSwap (BONE)		+3.40%	-19.41%	-45.58%	$200.95m
8	Saddle Finance (SDL)		+2.61%			$144.59m
9	DODO (DODO)		+1.18%	-18.73%		$100.47m
10	DerivaDEX (DDX)		-0.14%	+8.80%	-1.61%	$63,486,063

Figure 4.2: List of top 10 decentralized exchanges by total value locked (source: `https://defillama.com`)

Next, the final metric considered is the utilization of the protocol. This can be analyzed through the trading volume a given decentralized exchange has. In reality, trading volume is a function of the total value locked discussed above. In other words, the higher the total value locked the more traders are incentivized to trade on that exchange, given lower slippage. therefore the higher the trading volume. As a result, to make an efficient use of volume as a metric it must be used complementary to total value locked. For instance, only projects with both high TVL and trading volume are eligible for the analysis. Figure 4.3 shows the weekly volume of all dexes on Ethereum since early 2020.

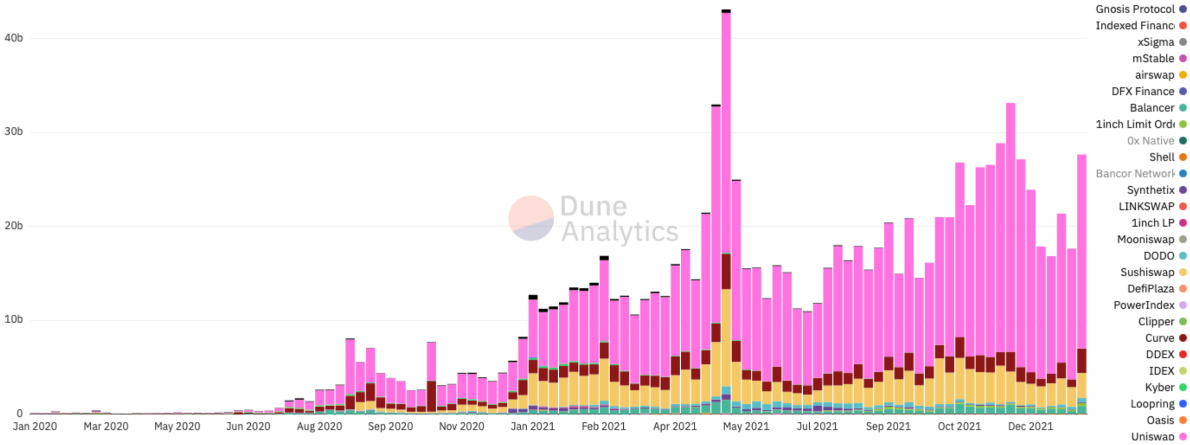

Figure 4.3: Weekly volume on all decentralized exchanges since January 2020

As visible, Uniswap, Sushiswap and Curve are the exchanges that have the highest trading volume Uniswap in particular holds nearly 70% of the weekly average trading volume, as visible in Figure 4.4. Moreover one can also notice, that these three exchanges together account for nearly 88% of the entire trading volume and 83% of the entire TVL. In conclusion, given that these three protocols are native to Ethereum, given their time in the space, and finally given the dominance they have in the market in terms of both total value locked and volume, Uniswap, Sushiswap and Curve will be the three projects analyzed in the following research.

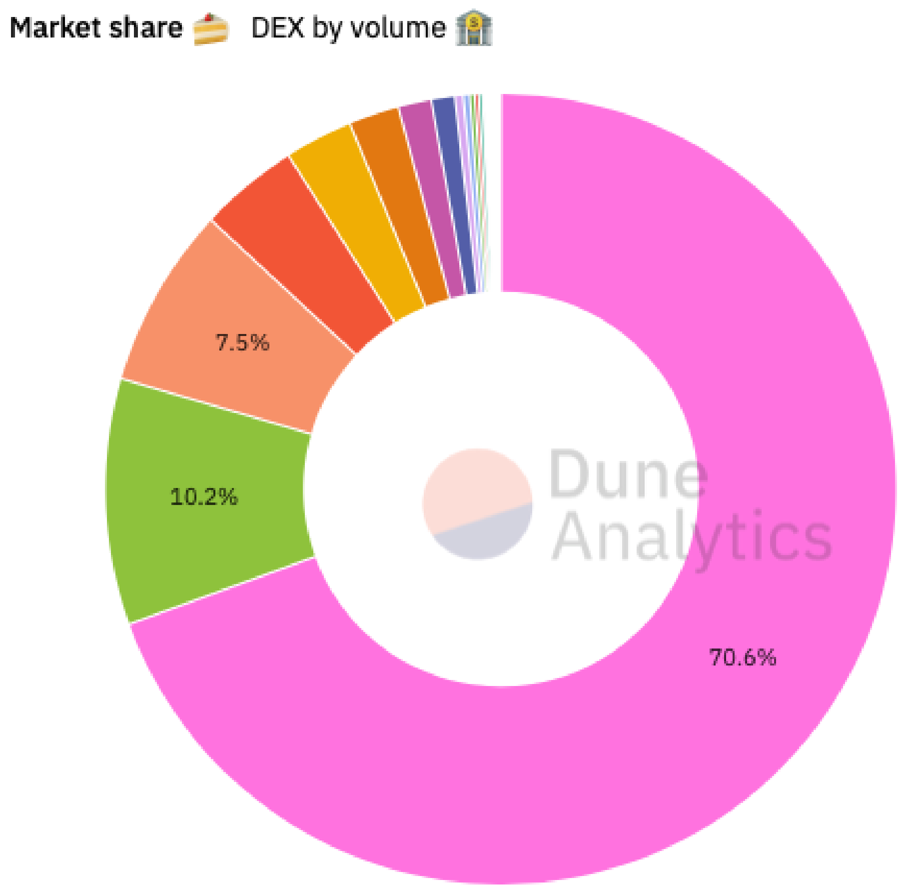

Figure 4.4: Decentralized exchanges weekly market share by volume

4.3. Data acquisition

As discussed in the research outline, the goal of the following research is to analyze the governance of the digital communities forming around decentralized exchanges, with the Institutional Analysis and Development framework developed by Ostrom (1990). In order to analyze her communities of interest, Ostrom used to spend long periods of time in their company collecting data and information regarding their rules and means of coordination. These communities were usually located in remote areas that were of difficult reach, therefore overcoming cultural and language barriers were also among the reasons of her prolonged stays. On the other hand, the digital communities that will be analyzed in this research are stateless by definition and are not bound to any geographical location. Furthermore, participants interact almost exclusively through online platforms and more often than not in anonymous fashion. As a result, the methodology for acquiring data and knowledge on these communities and on how they coordinate must be fundamentally different from the one implemented by Ostrom. The following section will cover the data acquisition mechanisms utilized while answering to the second sub research question *'How and what data can be retrieved for implementing the Institutional Analysis and Development framework?'*.

Fundamentally, public and permissionless blockchains like Ethereum are record of transactions that are shared among all the validators and visible to anyone. This implies that, for every application that runs on Ethereum, for instance, all transactions executed by such application can be monitored and audited by any participant. To provide an example, Figure 4.5 below shows the record of transactions of the Uniswap protocol over ten minutes. This data is publicly available on the Etherscan platform[1] and one can search for every transaction dating back to when the protocol launched.

Txn Hash	Method	Age	From		To	Quantity
0x8c178ae29f35f1f2407...	0xd66decf8	4 mins ago	Uniswap V3: UNI	→	0x51399b32cd0186bb3...	1,799.990559918496053475
0x62b8c5c9ea1e87bb7...	Transfer	5 mins ago	0x7773adb3dfd9633a5e...	→	OKEx	99.999999999999999999
0x7c9c55f399fa32c30f3...	Transfer	6 mins ago	Poloniex 4	→	0x2f75c3c399acd802c5...	902.80198245
0xd193da014ef5d0bd95...	Transfer	6 mins ago	Binance 16	→	0xf24c609e942a65efa7f...	1,834
0x521384df4717222a0d...	0xd6e13002	6 mins ago	0x9d406c4067a53f65de...	→	Uniswap V2: UNI-ISLA	61.251696735921978628
0x9813fce66616b3471f...	Flush Forwarder ...	8 mins ago	0x799dfd4083a146d3b3...	→	Bitstamp 2	571.98
0x07975d14e7a2a72e4f...	Transfer	9 mins ago	0x59e0cda5922efba00a...	→	0x799dfd4083a146d3b3...	571.98
0x0a000244d59685e7e...	0x2e2d726c	10 mins ago	0xe99bfe725ceddcf03d...	→	Gemini 4	311.72150194

Figure 4.5: Visualization of the record of transactions of Uniswap on the Ethereum blockchain over 10 minutes (source: `https://etherscan.io`)

As visible from the Figure 4.5, the following data points are available: the transaction hash which is a unique identifier for every transaction validated and added to the blockchain, the method, which indicates what type of transaction was performed (transfer, deposit, withdrawal), the age of the transaction, the sender and recipient of the transaction and finally the amount that was sent.

All of the data points listed above provide useful information on the performance of the exchange, for instance on its trading volume and total value locked. Nonetheless, the data retrievable on Etherscan is in raw format, meaning an additional platform is needed in order to fetch the data and perform analytics and data visualization. For this purpose, a number of data analytics platforms were utilized. Of these, the most useful and flexible for the analysis conducted was Dune analytics[2]. In simple terms, Dune extracts all the raw data produced by the Ethereum blockchain (among others) and aggregates it into a Postgres SQL database, which allows users to easily query the exact data needed. Furthermore, having the data in simpler format, Dune also allows analysts to perform data visualization techniques. Figure 4.6 and Figure 4.7 show first the backed architecture of Dune, and second the interface with an example for users to query in SQL and then visualize the data.

[1]Retrieved on 02/12/2021 on`https://etherscan.io`
[2]Retrieved on 02/12/2021 on `https://dune.xyz`

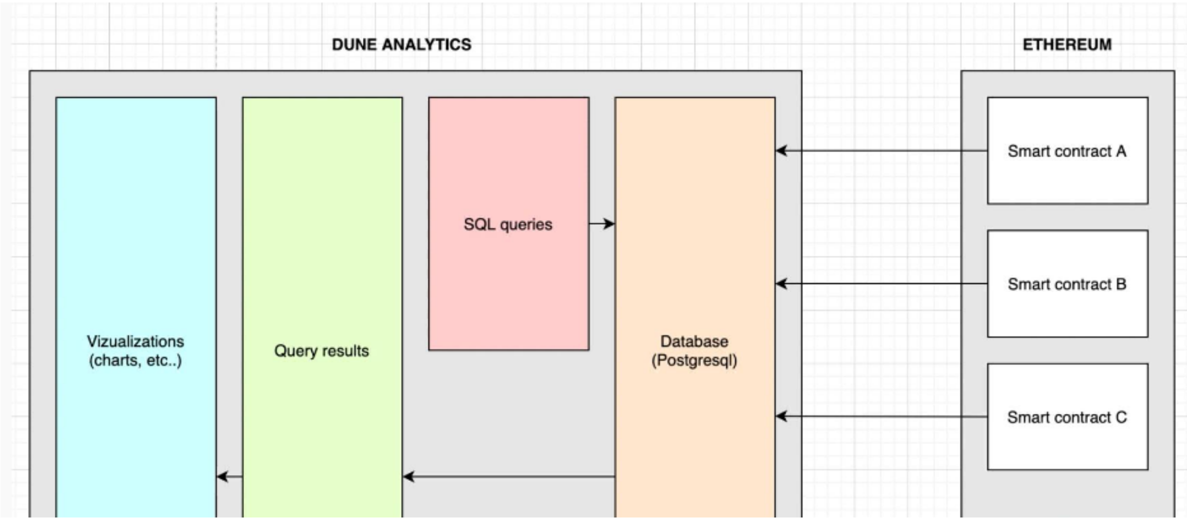

Figure 4.6: Dune analytics high level back-end architecture (source: `https://docs.dune.xyz`)

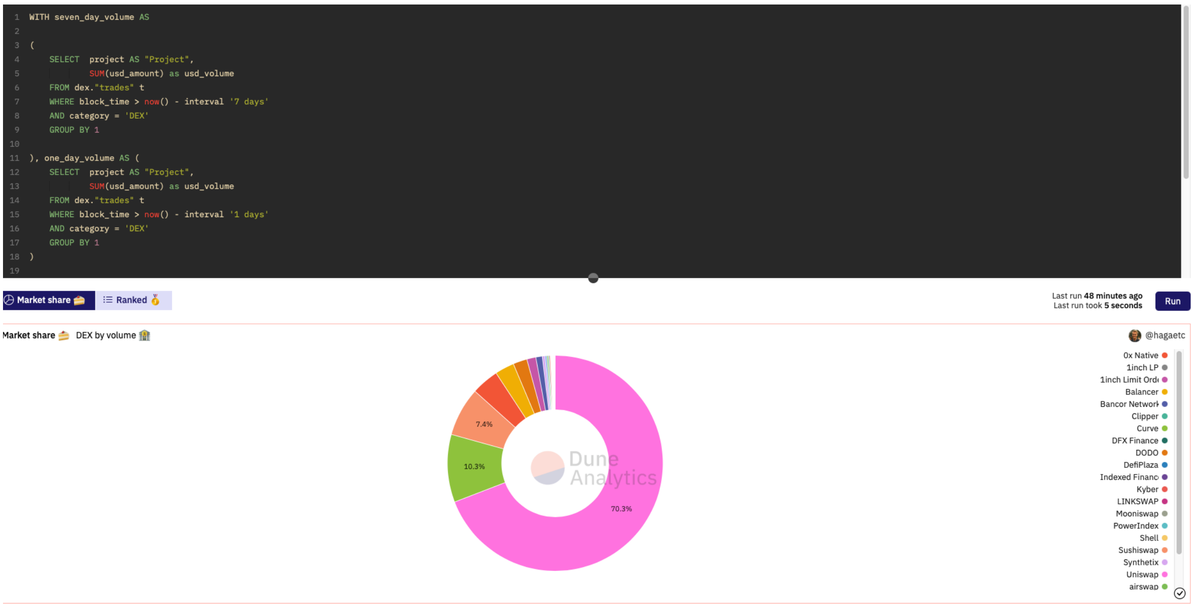

Figure 4.7: Dune analytics interface for data query and visualization (source: `https://dune.xyz`)

The two other platforms utilized for analysing data regarding the different exchanges are Tally[3] and Sybil[4]. Unlike Dune that allows users to query and create different visualization solutions, Sybil and Tally are simply data analytics platforms that provide ready visualizations and have a particular focus on the governance of the protocols. For instance, on Tally it is very simple to visualize the amount of participants that voted for certain proposals and their relative votes. Moreover, given that some of the addresses containing large amounts of tokens are doxxed (publicly revealed, not anonymous), these platforms also allow one to visualize the owners of certain addresses, unlike Dune. Figure 4.8 is an example of the tally interface, as visible, Tally makes it simple to visualize the voting power of participants over time as well as who some of these participants are. For instance, a16z is one of the largest venture capital funds in the blockchain space.

[3]Retrieved on 02/12/2021 on`https://www.withtally`
[4]Retrieved on 02/12/2021 on`https://sybil.org`

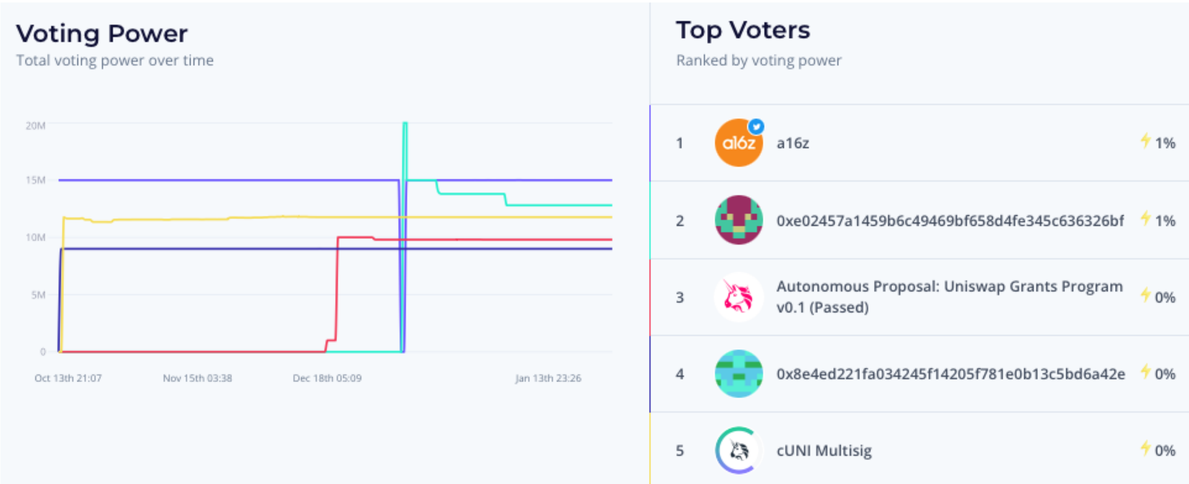

Figure 4.8: Voting power over time and largest Uniswap token holders (source: https://www.withtally.com)

4.4. Institutional Analysis and Development framework

The following section will discuss the main building blocks of the IAD framework as it will be utilized to analyze the projects that will be selected in the following sections. The framework, as represented in Figure 4.9, is built as follows. Central in the IAD is an action situation which relates to a particular coordination problem between users. The action situation is influenced by a set of external variables which comprise: biophysical conditions, attributes of the community and rules in use. External variables impact action situations and generate a set of patterns of interactions and consequent outcomes which are then assessed based on evaluative criteria set a priori. The latter are then utilized as feedback for the starting external variables.

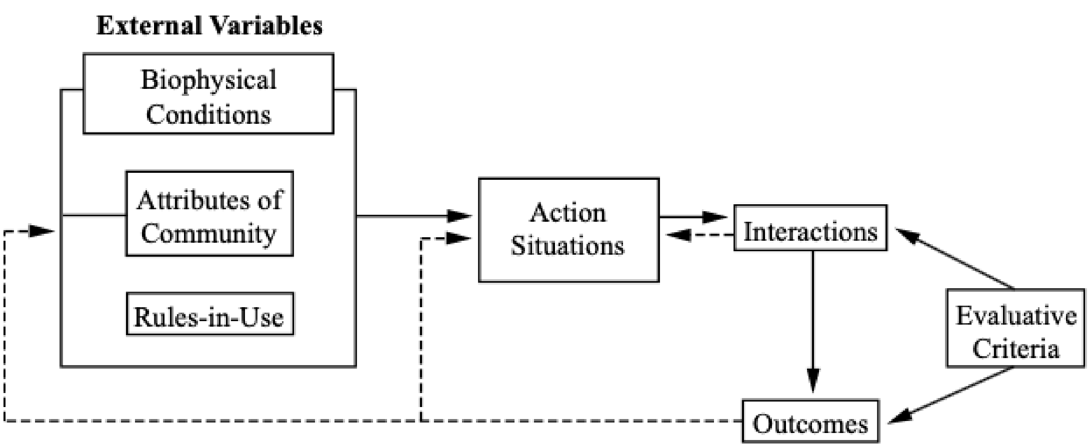

Figure 4.9: Institutional Analysis & Development framework (Ostrom, 2010)

Given that the IAD framework was developed mostly in the non digital era, there are a number of considerations to be made in order to utilize the framework for analysing patters of interactions of purely digital communities.

External variables

Biophysical conditions: according to Ostrom (2010), biophysical conditions can be often simplified as one of the four types of goods. In the specific case of this research, the governance of DeFi projects is non excludable (given the permissionless nature of the Ethereum blockchain), but highly rivalrous, as the amount of governance tokens is finite and whoever possess more of them has higher voting power. Also, as explained in the previous chapter, decentralized finance protocols simulate the actions that current financial intermediaries do (matching borrower and sellers) but they do it in decentralized and autonomous fashion. Liquid capital, hence becomes a common pool resource.

Nevertheless, other than classifying decentralized finance in one of the four types of goods, the following research will categorize biophysical conditions also based on the characteristics and technical specifications of the blockchain itself. Given that the protocols that will be analyzed in the following research are all built on the Ethereum blockchain, the 'biophysical' conditions, or perhaps better labeled as 'bio-digital conditions', will be the ones pertaining to that specific blockchain.

Ethereum is an open source, public and permissionless blockchain. Its founder, Vitalik Buterin, understood back in 2014, that blockchain could be used for more than just money, as for the Bitcoin case. Therefore, he developed a blockchain with a dedicated scripting language (solidity) that could be used as digital infrastructure for building decentralized applications, Ethereum (Lubin, 2014). Ethereum holds all the major characteristics necessary for building a decentralized and trustworthy digital architecture. It is permissionless by nature, meaning anyone with a terminal and internet connection can connect to the network and even run a node. This of course makes it non excludable and decentralized as anyone around the world can be forming part of it. The blockchain is also public which signifies that all the transactions are transparent and instantly auditable by anyone being connected to the internet. Last but certainly not least, Ethereum introduced smart contracts, which are code that can execute any type of transaction following given conditions (Buterin, 2014a). This is what gave birth to the concept of programmable money. All of the mentioned characteristics of Ethereum are what make possible the creation of Decentralized Autonomous Organizations (DAO) (Buterin, 2014b).

This type of network design bring a number of advantages. First and foremost, the fact that it is censorship resistant and can be accessed by anyone, democratizes its use. Furthermore, since transactions are processed by transparent and auditable smart contracts, using the platform requires a lower degree of trust with respect centralized or traditional exchanges where transactions are not transparent are overseen by humans which are prone to opportunism (Williamson, 1979).

Attributes of the community: as for the attributes of the community, DeFi communities are very rare and the first ones of their type. They are heterogeneous in the sense that these communities are formed by people coming from all over the world with an age range that spans from (tech savvy) adolescents to senior developers which have many years of experience in computer science. On the other hand, these communities are homogeneous in the sense that all users share at least a basic technical understanding of blockchains, its technical characteristics and speculative nature. DeFi communities are hence formed by core developers, early investors and application users, which are usually also developers.

For the specific protocols being analysed users can be classified into liquidity providers (LPs), traders and developers. Liquidity providers are incentivized to deposit liquidity in the protocol in exchange for economic rewards. LPs can simply be token holders that wish to earn passive interest on their capital, or they could also be professional market makers that constantly deposit and withdraw their capital from different protocols

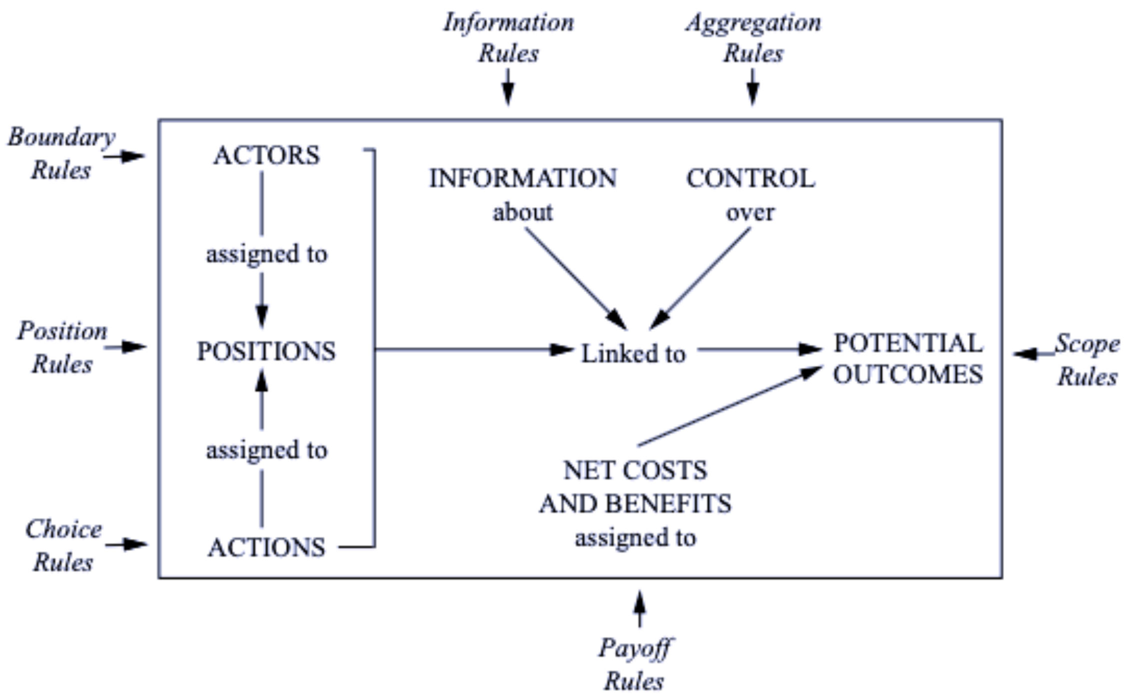

Figure 4.10: Rules in use of the Institutional Analysis and Development framework (Ostrom, 2010)

looking for the best yields. The trader category can also be further subdivided. These can be speculators, which are individuals with profit maximising strategies regardless of the underlying technology. Arbitrageurs, which are much needed in order to keep the price of a certain asset equalized across different platforms and finally, other decentralized application users that buy tokens in order to utilize them on their own platforms.

Rules in Use: these are the third and final factor of the external variables. According to Ostrom (2010), the rules in use delineate the guidelines for those involved in the action situation on who must not or must take a certain action. Its important to clarify that rules in use do evolve over time as the action situations may vary themselves according to different parameters. During her extensive multi decade research, Ostrom found an incredibly wide array of rules utilized for coordinating communities and one of the main challenges was to code and organize all these rules into logical clusters. As visible in Figure 4.10, a total of seven different types of rules operating as external variables were identified.

1. *Boundary rules* specify the means and conditions by which actors can enter or leave the action situation. These rules will obviously have an impact on the total number of participants and on their ability to leave and enter the action situation multiple times in time. For the specific case of DeFi protocols, given their permissionless nature, boundary rules appear to be relatively lax. In theory, participants are able at any time to deposit and withdraw their capital with no lock up periods. In reality, at the time of writing, the non user friendly interfaces and the possibly high fees on the congested Ethereum network (scaling solutions are underway) are presenting quite some entry barriers for new users to be on boarded. While innovations in the following months will most probably smooth these aspects, they do represent a difficulty that only the tech savvy are willing to overcome.

2. *Position rules* specify what are the different positions actors can hold in the given situation and how

many actors hold each position. For the case of decentralized exchanges (dexes), as will be better explained in the next chapter, the main positions held by different actors are (i) being a buyer or a seller of a given asset and/or (ii) being a liquidity provider, providing capital to the smart contract for facilitating exchange between other transacting parties.

3. *Choice rules* specify the available set of actions that actors can take by being in a certain position. In decentralized exchanges, transacting parties can either buy or sell, choosing both the price and the fee they intend to pay. While liquidity providers, can choose the amount of liquidity they wish to supply and the amount of time they wish to supply it for. That is, no lock up periods.

4. *Information rules* specify what information must or must not be shared by participants in a certain position, as well as the channels of communication for doing so. Given the public nature of the Ethereum blockchain - meaning anyone from participants to non participants can see the data on the functioning of the protocol - most of the relevant data required by participants to reason and take action is available and transparent.

5. *Scope rules* delimit the possible outcomes that could be affected by the unravelling of the action situation. Moreover, they try to link actions to their relative outcomes.

6. *Aggregation rules* are relative to the degree of control that a certain participant in a given position can exercise to decide on what action should be taken. In other words, aggregations rules determine the power and freedom a participant has in choosing his own actions.

7. *Payoff rules* specify the costs and benefits that should be assigned to actors following a certain combination of actions and outcomes. In other words, these rules define the incentives and deterrents for sets of actions.

Action situation

In accordance to Ostrom (2010), action situations involving participants, their possible actions and relative outcomes, can be analyzed on three distinct layers: (i) operational, (ii) collective choice and (iii) constitutional level. Operational rules set how individuals and the network should work during daily operations. For blockchains, hence DeFi protocols, these rules are hard coded into the protocol and overseen by the nodes of the network. On this level, blockchains work as self-governing systems that decides which transactions (actions) are valid and which are not based on how the protocol is configured. Collective choice, or policy, rules in use are the ones that regulate the process under which operational rules are made. So to speak, collective choice rules function at a higher level with respect to operational rules as the former define the latter. These are the most common set of rules that are currently being decided upon in most of the DeFi communities. Members vote and try to reach consensus on topics relating to the operational features of the protocol as: which assets can be traded on the platform, what are the fees and the rewards for providing liquidity. Finally, constitutional rules function at the highest level of the three as they govern the process of deciding who can participate in making collective choices. Given the permissionless nature of the decentralized applications discussed in this paper, constitutional rules are virtually non existent as literally anyone can join the community and propose and vote on given proposals. However, the way governance tokens are distributed and their weight in the voting process are critical characteristics for a fair and equitable community governance. Therefore, such characteristics belong to the constitutional rules set.

As mentioned earlier, these external factors will impact action situations and realize patterns of interaction and certain outcomes. It is to note that in the voting processes of the various DeFi models, rules which are decided upon can be either policy or constitutional ones as operational rules are followed and executed exclusively by the protocol. The action situations discussed in this research will mostly refer to how the community manages (or not) to reach consensus over a certain proposal. This will be influenced by the distribution of governance tokens, the thresholds set for reaching quorum and proposal passing or rejection, the incentives given to users to participate in governance and finally the actual involvement of the users.

Evaluative criteria

In order to evaluate whether a certain protocol (smart contract) is successful or not, institutionally speaking, a number of quantitative evaluative criteria were thought of an elucidated below. Given the publicness of the blockchain, much of the data was relatively simple to retrieve through 'on-chain' analytic platforms as Dune Analytics [5]. One of the first metrics to be considered is the amount of liquidity pooled into a certain protocol, also known as total value locked (TVL). The higher the trust by users on a certain protocol, the more these users will trust the protocol with their funds, hence a higher TVL. The TVL can therefore be a metric on the sentiment and trust the markets has on the project. Nonetheless, there are some cases where protocols incentive users, for certain amount of periods, to deposit capital in their protocols in exchange for financial incentives. This means, that certain TVL spikes can be caused by incentives more than by trust and actual development (Stepanova and Eriņš, 2021). Usually, as incentive periods terminate, the TVL decreases accordingly. These factors are taken into account.

Next, protocols are evaluated based on the distribution of their governance tokens and their availability to retail investors. As mentioned earlier, most protocols utilize 'one token one vote' mechanisms for reaching quorum or consensus over a proposal. This implies that users with high amounts of tokens have a higher voting power which can potentially lead to centralization of decision making power. Different protocols adopt different mechanisms to prevent such centralization and will be better discussed in the next chapter. Accordingly, protocols with more fair distribution mechanisms will be regarded as more decentralized and democratic, hence better.

Governance mechanisms such as quorum and proposal thresholds are also parameters considered to evaluate the degree of success of given protocols. Projects with high proposal thresholds make it virtually impossible for small retail participants to make proposals or even have relevant weight in decision making. This is the case for the Uniswap project which will be better explained in the next chapter. A number of developers and venture capitalists in the space point out that at very early stages of development as the current one, centralization of decision making power is the fastest and most secure way for growth and adoption, as only the core developers have the actual real understanding of the development process and have at heart the protocol's success. While these are valid arguments and certainly true for a number of projects, others have taken advantage of these mechanisms to grow personal wealth and power over the protocol (Rekt, 2021).

Finally, it is crucial to understand whether the communities are actually vibrant and involved or if users accrue tokens purely for economic incentives. Protocols where users see governance tokens mainly as yield will tend to have lower community involvement (voter apathy) and as a consequence a sub-optimal governance. Successful projects are the ones that manage to align both financial and governance incentives for users in the interest of the protocol's long term sustainability.

[5] Retrieved on 13/03/2021 `https://duneanalytics.com/home`

5

Analysis

The main aim of the following chapter is to analyze the selected decentralized exchanges with the Institutional Analysis and Development framework developed by Ostrom (2010). The chapter will expand as follows: first, the external variables for decentralized exchanges will be investigated, followed by an establishment of both the action situation being considered and the evaluative criteria formulated and utilized for assessing the different projects and their ecosystems. Finally, each of the decentralized applications will be dissected in the institutional sense and, with the use of on and off chain data analytics, evaluative criteria will be compared in order to answer the research question and sub-questions.

5.1. External variables

The following section will examine all of the external variables of the IAD framework, namely (i) biophysical conditions, (ii) attributes of the community and (iii) rules in use, in relation to the use cases being discussed. For the sake of clarity, Figure 5.1 below illustrates once more the key building blocks of the framework.

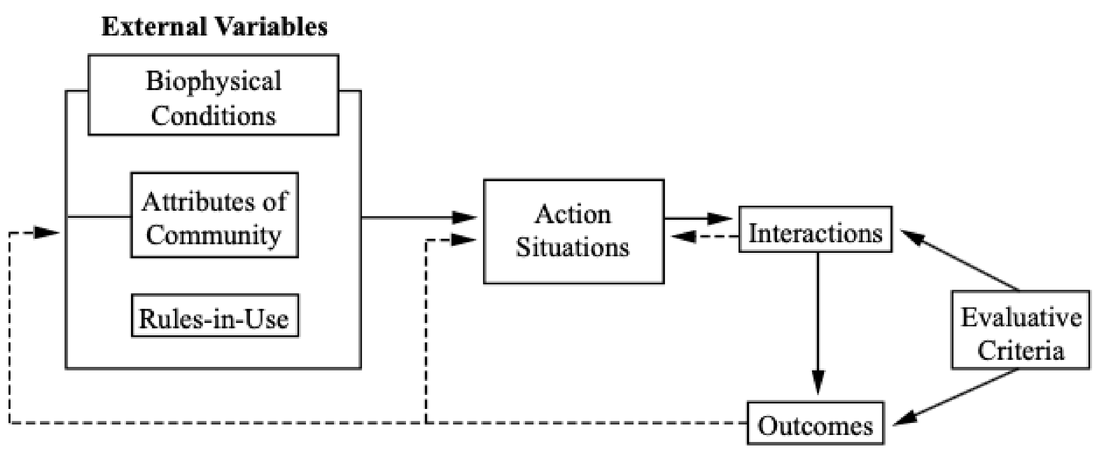

Figure 5.1: Institutional Analysis & Development framework (Ostrom, 2010)

Biophysical conditions

Following the theory developed by Ostrom (2010), biophysical conditions are the attributes of the physical world that affect the variables in an action situation. In other words, they define the boundaries of what is physically possible and the potential resulting outcomes. As discussed in the previous chapter, two of the attributes most frequently utilized for describing certain conditions are: excludability and rivalry. Therefore, it makes sense to utilize these two attributes for a first categorization of the topic in discussion: the governance of decentralized exchanges. As explained in the research outline, the protocols selected, as well as the vast majority of the protocols developing decentralized financial applications, utilize governance tokens to confer governance rights. As these tokens are available for anyone to buy, hold and trade they are by definition non excludable. In other words, anyone in possession of capital and an internet connection is capable of accumulating governance tokens, and as a result, governance power. On the other hand, the supply of these tokens is capped, meaning there is a finite amount of tokens in existence. Therefore, the tokens and the governance rights deriving from them have a high degree of rivalry. As will be better explained in the following sections, this holds particularly true for the protocols that utilize a one token one vote mechanism like Uniswap (Bulat, 2018).

Participants with large amounts of capital are incentivized to accumulate (buy) more tokens as possible as this will grant them higher voting power in governance proposals. This can in turn lead to centralization of power and stagnant governance communities. Different projects utilize different mechanisms for mitigating these risks, as for instance the time-weighted voting system introduced by Curve (Egorov, 2019b), which will be discussed in detail in the next sections. Following the discussion above, it becomes theoretically correct to claim that the governance of these protocols can be treated and considered as a common pool resource given the combination of low excludability and high rivalry. Nonetheless, on chain data retrieved and analyzed suggests that while this might hold true in theory, in practice these protocols are currently resembling corporate (hierarchical) governance to a larger extent.

Other than the first and over simplified categorization discussed above, one may wonder what exactly are the biophysical conditions for a protocol that purely exists as code written in the digital realm. In other words, if the biophysical conditions are the externalities imposed and enforced by the laws of physics in the real world, what then are their digital equivalent?

In order to answer this question it is first necessary to provide a bit of context and adopt a wider perspective. The first successful implementation of blockchain technology was Bitcoin, officially released in early 2009. However, it is important to understand that the concept of blockchain - intended as the cluster of technologies that enable a decentralized autonomous network - was born only after the launch of Bitcoin. As a matter of fact, the term 'blockchain' never appears in the Bitcoin whitepaper (the 'formal' document explaining its purpose and technical specifics) (Nakamoto, 2009). The Bitcoin network and its currency (bitcoin) were invented for a very specific purpose, to have a digitally native currency and payment system free from financial intermediaries. Until that point in time, payment systems on the internet were simply digital extensions of 'terrestrial' financial intermediaries, also known as 'fintech'. The rationale for developing an independent and digital monetary system was: if communication systems have evolved independently into digital ways of exchanging information - such as emails and the many messaging applications available today - so must monetary and payment systems. After all, as explained by Hayek (1945), price systems are a mechanism to transfer information about supply and demand of goods and services.

With that goal in mind, the pseudonymous inventor(s) 'Satoshi Nakamoto' combined together a series of technological advances: Public Private Key cryptography for transaction encryption, a Byzantine fault-tolerant consensus algorithm for synchronizing state updates on all the nodes of the network (proof of work), a peer to peer network for connecting participants and finally, a digital currency (Nakamoto, 2009). The genius and success of this particular protocol were immediately evident to a good number of developers and cryptographers of any sort, such that many started to research whether a this new type of technology could be used for more than just a digital currency payment network.

Practically speaking, developers now faced an interesting dilemma. They could either build applications on top of the Bitcoin blockchain or build an entirely new blockchain from scratch. Both solutions came with their own set of difficulties. Building on top of Bitcoin meant constraining oneself to the technical specifications of that particular blockchain as: limited set of transaction throughput, limited data types, limited data storage sizes and even having to utilize a pretty unique and constrained programming language called Script. On the other hand, building an entire new blockchain from scratch implied an enormous workload as bootstrapping all of the elements of the infrastructure and extensive testing.

From this particular conundrum, in 2014, a nineteen year old programmer named Vitalik Buterin started developing the idea of creating a general purpose blockchain (Buterin, 2014c). The goal was to develop a protocol over which developers could build with far less constraints. Eventually, in mid 2015 he launched Ethereum. The value proposition of Ethereum was pretty simple, other than the sets of technologies mentioned above (consensus algorithm, encryption systems, etc) it also ran a built-in 'Turing complete' virtual machine, therefore capable of executing code of any logic and complexity and solving any computable problem. Moreover, the chosen programming language was Solidity, an extension of the well known Java programming language, therefore attracting and making it easier for a wider range of developers to build on Ethereum. This eventually created the perfect conditions for blockchain enthusiast to easily build decentralized applications without having to worry of building everything from scratch and by using a more familiar scripting language.

Even though many other project tried to do what Buterin did, Ethereum had the first mover advantage such that as of today, around 6 years after its launch, the very majority of decentralized applications are built on top of it. By looking at it through this perspective one can define the technical characteristics of Ethereum as the 'biophysical conditions' that underline and at the same time make possible, the flourishing of governance for decentralized communities. For clarity, Figure 5.2 below illustrates the architecture behind building decentralized applications.

Each layer builds on top of the other. Given the open source nature of most of the Ethereum ecosystem, this creates an open and composable infrastructure that allows anyone to build and connect to other applications. This is also one of the main reasons behind the dramatic growth experienced in the last couple of years. Furthermore, it is key to understand that these layers are hierarchical, meaning their security is dependant on the layers below. If one of the layers were to be compromised, so would be the layers on top of it. In the same way, if one were to build a permissioned layer as foundation, then applications built on top of it would not be able to achieve true decentralization.

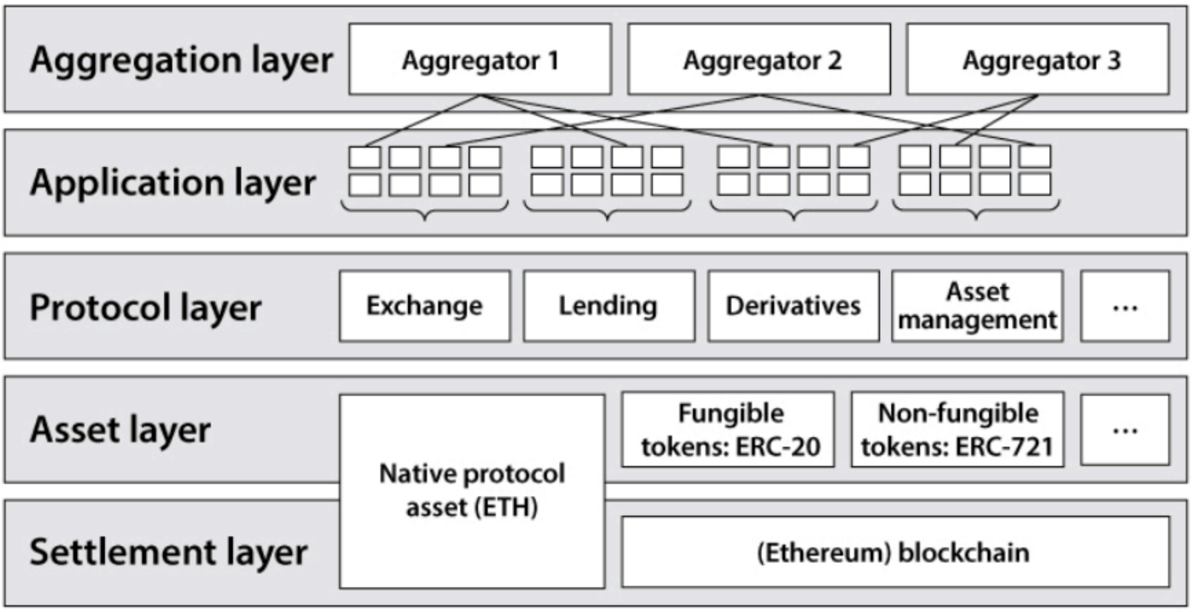

Figure 5.2: Decentralized finance building blocks (Schär, 2021)

The five layers that form the infrastructure are:

1. The settlement layer is basically the blockchain itself comprising consensus algorithm, ledger transaction records, reward systems and the native asset of the protocol. This is the layer where transactions and settlements occur. Examples of this layer are obviously the Ethereum blockchains with its native asset Ether, and the bitcoin blockchain with Bitcoin as native asset.

2. The asset layer comprises all the assets which can be deployed on top of the settlement layer. This is where one can build tokenized assets whether real world or digitally native.

3. The protocol layer is where bundles of open source smart contracts create the standards for use cases as decentralized lending markets, decentralized exchanges or derivatives markets. Again, given that the vast majority are open source, these smart contracts are highly composable and interoperable, thus accelerating development speed.

4. The application layer is where the smart contracts developed in the previous layer are utilized to build user oriented applications. Users typically interact with smart contracts through browser user interfaces which are developed at this layer.

5. The aggregation layer is somehow an extension of the layer below, where given the high composability and interoparability mentioned earlier, applications are built for users to interact seamlessly and simultaneously with different applications.

Attributes of the community

As explained in the previous chapter, one can categorize the participants of decentralized exchanges into three main clusters. The first cluster is formed by the core developers that built (coded) the protocols and constantly oversee their correct functioning. As will be discussed later, core developers are the ones that set the rules in use at every level from operational to constitutional. Nonetheless, through governance mechanisms the power of proposing and changing rules transfers in time to the overall community through governance tokens. Different projects adopt different models of token (power) distribution and will be the main focus of the next sections. Next to core developers, another set of participants are liquidity providers which supply assets to both sides of the pool in return for trading fees. A number of liquidity providers can be regarded as 'early adopters' as they were among the first to provide liquidity to these smart contracts. Such liquidity providers, or investors, obviously had a high understanding of both the technology and the risks involved in interacting with early stage smart contracts. Before delving into the next set of participants, it might be helpful to highlight that both early developers and early liquidity providers shared (and still do) the same ethos, to build transparent, inclusive and decentralized financial services. These are pretty much the same values that shaped the views of early developers and cryptographers that kick started the blockchain ecosystem nearly a decade earlier.

The third set of participants are the users of decentralized exchanges, the ones that utilize liquidity pools to transact one asset for the other, in financial terms, 'traders'. On one hand one could further categorize these participants as merely users or clients of the network, as they rationally decide to trade on decentralized exchanges rather than on their centralized competitors based on pure financial efficiency. Nonetheless, traders can also accrue governance tokens and form 'alliances' between them in order to grow in governance power and try to steer the protocol in directions more favourable for them. As a result, as data will prove later, traders must be considered in many situations as active governance participants.

Other than core developers, liquidity providers and traders, two out of the three projects analyzed have also a fourth key participant which are venture capital (VC) firms. The goal of these firms is to fund projects early on in exchange for equity, stake in the project. For core developers this is ideal as they are provided with substantial amounts of capital and resources in order for them to continue building, while for VCs the advantage is to be able to acquire large amounts of equity at very low prices, hoping to sell it in the future at many multiples. In decentralized finance, equity is often given to early investors also in the form of governance tokens. For projects and startups in many industries this is a very common form of raising capital. Nonetheless, the presence of venture capital firms also has an impact on the governance of the project itself. Given that VCs deploy substantial amounts of capital, they want to make sure the project goes in directions where their investment is likely to grow. As a result, this can potentially translate in governance pressure on core developers and a series of reactions from both liquidity providers and traders that are sub-optimal for the project itself.

As these protocols have grown and proved resilience to exploits and unfavourable market conditions, the amount of traders and liquidity providers have incredibly increased over time, particularly from mid 2020 to date (`https://dune.xyz`. To put things into perspective, as visible in Figure 5.3 below, the amount of users has increased nearly twentyfold in the span of nearly a single year. However, this does not directly translate to a likewise increase in governance participants. As proven many times in the last decade, crypto assets can be extraordinary speculative vehicles, this is no different for governance tokens of decentralize exchanges, or other decentralized applications. As a matter of fact, a wide number of speculators buy and sell governance tokens without evening knowing that by owning them they would have access to governance rights and decisions. As a result, protocols have put in place rules for becoming a governance participant. In other words, it is not sufficient for a participant to hold a governance token in order to participate in governance, there is a set of boundary rules he should abide to, as will be discussed in the next section. While it is true that significant speculation is hardly something good for any sort of asset, as it impacts heavily the perception of market participants, one also has to recognize that surviving speculative cycles increases the resilience of the projects that have strong fundamentals and strong communities, in other words becoming 'antifragile' (Taleb, 2012).

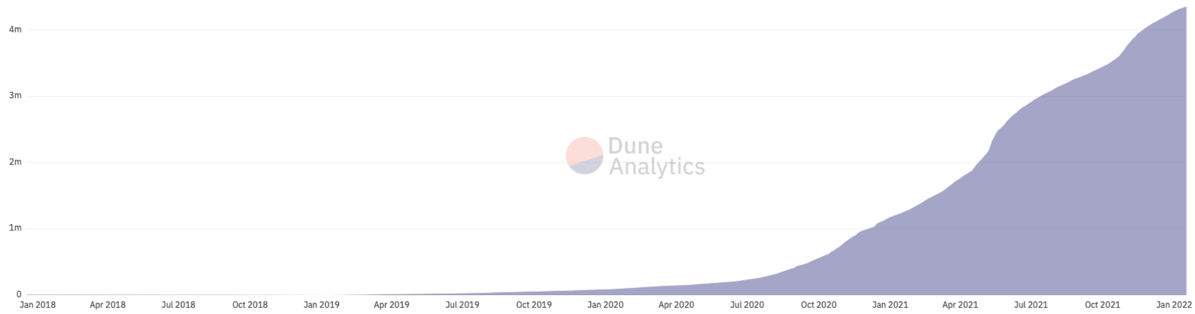

Figure 5.3: Cumulative DeFi users since 2018 to January 2022

Finally, it is worth pondering on the human composition of these communities. Since the advent of the internet, and more specifically of social media, humans have had the ability to join geographically unbounded communities. In other words, before information technologies, one would become member of local communities as local sports associations and religious communities. Today, one is capable of virtually joining communities of people having the most diverse backgrounds and cultures. What creates communities is usually a common interest. As outlined above, early stage community members of decentralized exchanges shared mostly the same core perspectives of financial freedom. While these type of members grow by the day, so do member that have return on investment (ROI) as sole scope, however the latter disappear or loose a great deal of interest once markets surpass speculation bubbles. Therefore, it is participants that share ethos which endure in the communities and eventually shape its trajectory in time. In this way one can claim that decentralized finance communities are homogeneous in the sense that the very vast majority of early and key community members share not only the same values but also a very similar and in depth understanding of the complexity of the technology and its broader implications (Joseph, 2019). However, they are also heterogeneous in the sense that they are formed by people of different ages, nationality and social class spread around the world. Many participants are traditional developers with decades of experience that are willing to share their knowledge and experience. On the other hand, there is a good deal of younger members, from high school to university students, which quickly experience the impact they manage to have at a very young age with nothing more than a computer and an internet connection. As for geographical locations, the discord channels of the three main project discussed give an idea of the cultures and countries which are mostly involved.

Rules in use

Among the three sets of external variables that influence an action situation, rules in use are by far the ones that differ the most between projects. As elucidated above, both biophysical conditions and attributes of the community are pretty much the same for the projects that will be discussed. However, each protocol has its own specific set of rules that influence interactions and relative outcomes.

As discussed by Ostrom (2005), there are two different approaches for analyzing and classifying rules. The vertical approach studies sets of rules that are nested in other sets of rules defining how the first set should be changed and decided upon. This approach comprises three different levels of analysis. Starting from the bottom up, the first level of analysis are the 'operational rules' which are the rules that shape the daily decision making of participants in the action arena. For this particular research and for most decentralized applications, operational rules are the ones carried and enforced by the protocol itself. For instance, the particular steps one should take in order to deposit or withdraw capital from pools. In the case of a user having to deposit capital, the code will execute autonomously to transfer the users capital from its own wallet to the desired smart contract (liquidity pool), at the same time the network itself is responsible for updating every single node to the new state. As noticeable, operational rules in blockchain applications are per the vast majority self-enforcing (autonomous) and irreversible. The community itself does not manage nor execute tasks at the operational level. What communities can do, is to decide upon and change operational rules.

The second level of abstraction constitutes collective choice rules which, as defined by Ostrom (2005), influence operational activities and outcomes as they define who is eligible to be a participant and the rules to be followed to change operational rules. This, and the following, are the levels that will be discussed the most throughout the rule analysis of following sections. One important factor to mention is that for decentralized applications that run on public and permissionless blockchains as Ethereum, collective choice rules do impact operational activities directly but do not define who is eligible to use the protocol as, by definition, anyone with internet access should be able to exchange in decentralized market places like Uniswap, Sushiswap and Curve. Nonetheless, this is the level where governance participants decide upon various key parameters that influence the growth and success of the protocol. For instance, participants may decide whether to add certain asset pairs to be traded or to financially reward the liquidity providers of some pools more than others. All of these with the ultimate goal of increasing liquidity in the protocol, therefore increasing its efficiency and its usage, resulting in more fees distributed to liquidity providers.

Finally, the third and highest level of abstraction for rules is the 'constitutional level'. Constitutional level rules relate to collective choice the same way the latter relate to operational rules. Or in other words, constitutional rules influence collective choice rules in terms of who is eligible to be a participant and the rules to be used in outlining collective choice ones. As mentioned earlier, every project has different boundary rules, meaning different rules for granting participants access to given positions. A good example for this, which will be examined in depth later on, is how Uniswap and Curve differ from allowing a given token holder to become a governance participant. In the case of Uniswap, all the token holder has to do is to delegate his voting power to an address. This address could be himself, or any other participant that he feels in line with his views, in full representative democracy fashion. In the case of Curve, in order for a token holder to become a governance participant he must first lock his token in a contract for an arbitrary amount of time spanning from a week to four years. The longer the locking period the higher the granted voting power. This simple mechanisms is a safety measure for the governance of Curve as whoever wants to truly participate in decision processes must first commit both time and capital.

The other approach utilized for analyzing rules is the horizontal approach, which covers rules regarding: positions, boundaries, choices, aggregation, information, payoff and scope (Ostrom, 2005). As noticeable, each project implements different type of rules for most of these categories and for two of the three verticals presented earlier. As a result, one can argue that different rules lead to different types of interactions and different outcomes. The goal of the following sections of this chapter will be to scrutinize the rules each protocol implements and how are these able to determine their success or failure. Given that the state of development of these new governance mechanisms are still very early, many categories do not even have defined rules. Fortunately, Ostrom (2005) covered also this possibility during her multi decade analysis and outlined a series of rules which come in place by default when no proper rules are specified. These sets of default rules are better visualized in Table 5.1 below.

As one can infer, in open and permissionless communities where users are sparse around the world and often relate to each other in anonymous or pseudonymous settings, it is quite difficult if not impossible to set rigid rules that everyone should follow. Simply put, there is no guarantee that a set of truly unknown participants may behave as desired. Therefore, the best rule setters can do is to establish incentive and slashing mechanisms in order to influence the behaviour of participants. In other words, instead of dictating musts and musts not, for these type of communities it has proven to be way more efficient and practical to delineate the incentives of certain actions rather than others. The self enforcement and network update coordination provided by blockchain technology simply aids to this concept.

Default conditions	
Default position condition	One position exists.
Default boundary condition	Anyone can hold this position.
Default choice condition	Each player can take any physically possible action.
Default aggregation condition	Physical relationships present in the situation determine the aggregation of individual rules into outcomes.
Default information condition	Each player can communicate any information via any channel available to the player.
Default payoff condition	Any player can retain any outcome that the player can physically obtain and defend.
Default scope condition	Each player can affect any state of world that is physically possible.

Table 5.1: Default rules in use when no clear rules are define (Adapted from (Ostrom, 2005))

5.2. Action Arena

According to the official structure outlined by Ostrom (2005), action arenas are composed of two major holons being (i) participants and (ii) action situations. Participants can be regarded as the actors that play a given role in the arena and have already been analyzed in the previous section. Furthermore, participants in the action situation are assigned to given positions over which they detain a certain level of information and control. Later sections will provide a deeper explanation of what are the potential positions that can be taken in the governance of decentralized exchanges, the information available to participants and the means my which they are able to execute their control, among others. The second holon of the action arena is the 'action situation'. In Ostrom's (2005) definition, 'whenever two or more individuals are faced with a set of potential actions that jointly produce outcomes, these individuals can be said to be in an action situation'. Given that the following thesis focuses on new forms of coordination mechanisms provided by blockchains, the action situation of interest occurring in the protocols analyzed will be: the process by which all of the different participants reach (or not) consensus on proposed changes to the operational functions of the protocol, or to the collective decision making process itself.

5.3. Evaluative criteria

The following section will present and argument on the five different evaluative criteria that were selected in order to assess the performance of the protocol and their relative communities. With the advent of on chain analytics and platforms such as Dune Analytics[1] it is now possible to collect large amounts of data that enables one to track with ease and flexibility the desired performance indicators. The five selected criteria, which will be explained in detail as follows, are: total value locked (TVL), volume, community size, community involvement and finally, token distribution. This section answers to the third sub research question *'How are evaluative criteria defined and why?'*.

Total value locked

The total value locked (TVL) is perhaps one of the most followed metrics for decentralized applications. It is literally a measure of the value - usually denominated in US dollars - of the total amount of assets deposited into the liquidity pools (smart contracts) of a given project (Stepanova and Eriņš, 2021). It is worth recalling that smart contracts are 'simply' code that run on an open and distributed network and is therefore accessible to anyone. While this is a valuable feature in both theory and practice, as well as one of the core values of the space, it also means that it is at the mercy of hackers and highly skilled developers that interact with it in malicious fashion. Liquidity pools are smart contracts that act as financial escrows and perform operation based on what they are instructed to do. Given the earliness of the space, to date there have been a good amount of successful exploits that have managed to circumvent the safety measures of the contracts and as a result drain capital from the pools.

Moreover, projects are composed of many liquidity pools. For instance, there are as many pools as there are tradeable market pairs in the DEX. Each liquidity pool is a separate smart contract, a separate escrow. The TVL is an aggregate of the value of all these pools combined. This being said, when a malicious actor tries to steal funds from one of the pools, users of the other pools might be concerned with the fact that also their pool is at risk and might therefore withdraw funds. The TVL is therefore, to a certain degree, a measure of the trust that a community is granting to the protocol and its core developers.

On the other hand, pools that offer the most rewards are also the ones that manage to attract more capital. So, usually projects with high TVL are also projects that offer constant and attractive yields. Given that exit costs are incredibly low, exiting certain pools and entering others can be very easy and fast for users. Whether because of safety concerns or because of chasing higher yields elsewhere. As a result, protocols that manage to retain or even accrue their TVL over time are are protocols that can arguably be considered both safe and profitable investments. To date, all the decentralized exchanges deployed on Ethereum combined have locked $31.1 billion USD of which Curve, Uniswap and Sushiswap cumulatively hold 81.5% or $25.36 billion USD.

[1] `https://dune.xyz`

Volume

Trading volume is defined by the total number of assets that have changed hands on a given period of time (Lo and Wang, 2000). Given that protocols generate fees from traders swapping one asset for the other, the higher the volume the higher the revenue generated by the protocol. Protocols can also accrue their volume if they offer trading pairs that other protocols don't. For instance, until recently Curve only allowed trading between assets with relative stable value. While Uniswap and Sushiswap have always offered trading on pairs of non pegged assets, as ETH/DAI. As a result, the trading volume on Uniswap in particular, has always been significantly larger than its competitors, as visible in Figure 5.4 below.

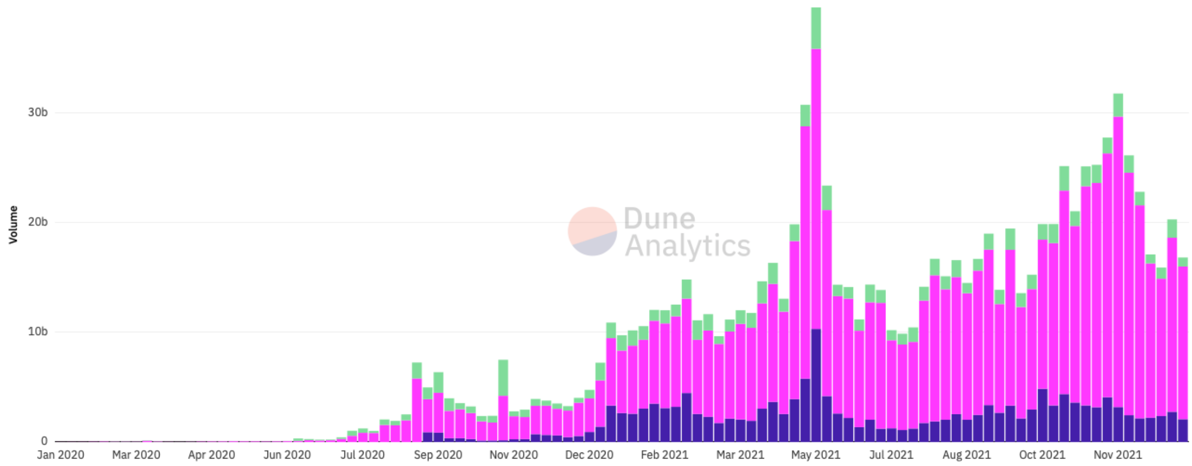

Figure 5.4: Weekly trading volume of Uniswap, Sushiswap and Curve from January 2020 to January 2022

Community size

The size of the community is also an important metric to determine whether the project is growing and getting traction or whether it is stagnating or loosing market share. As explained earlier, most of these communities have grown in the past year in the number of users given strong speculation. For this reason, this metric is particularly useful only if used in combination with the next metric which will be presented namely, community involvement. Analytics platforms today allow us not only to assess the number of users that have interacted with the protocol but also how many of them are actually involved in the governance process. This further allows analysts to quantify how much of the growth is due to speculation and how much of it is actually legitimate and interested in the actual development of the space.

Community involvement

As explained above community involvement is the criteria that will be utilized to determine what percentage of the community is actually involved in decision making, and what percentage is simply a user of the network. However, while the previous three metric namely, TVL, volume and community size can all be tracked for each project utilizing the same methodology (given that these are deterministic figures), in the case of community involvement, different methods for every project will have to be utilized in order to gauge governance participation. The reason for this is that each protocol utilized different boundary rules for users to enter a decision making position. Practically, this means that on different protocols users will have to perform different sets of actions in order access voting rights. For instance, in Uniswap users have to simply delegate their UNI tokens, while in Curve users have to first lock their CRV tokens in a separate smart contract. As a result, on chain analysis for community involvements differs project to project, as will be better elucidated in the following sections.

Token distribution

While the previous evaluative criteria aim at assessing the growth, trust and involvement of the different communities, token distribution aims at evaluating the degree of power centralization. As explained in previous sections, users must hold the governance tokens of projects in order to participate in decision making. In some protocols as Uniswap, each token corresponds to one vote. Other protocols like Curve, rely on both tokens and time in order to grant voting power. However, in all cases holding a token is always a necessary condition. This also means that users that manage to accumulate large amounts of tokens will consequently have a large voting power. By assessing the token distribution of each of the selected projects, one will therefore be able to determine if protocols are subject to entities having outsized voting power, and can therefore easily manipulate decision making. In other words, token distribution gives a measure of plutocracy in the governance of the protocol. This can be the case of projects that have received investments from VCs, which in return received large amount of governance tokens. Given that each of the selected projects utilize governance tokens in different ways in order to confer voting rights, like community involvement, token distribution is a metric that will be analyzed differently for each project.

5.4. Uniswap

Uniswap launched in November 2018 and is to date the largest decentralized exchange in terms of volume and user base[2]. It began as a side project for its founder, Hayden Adams, nearly a year before its official launch. Until that moment in time, most decentralized exchange projects had been trying to replicate order book models on chain with little success, given both liquidity and other technical constraints. What made Uniswap innovative and the center of attention was that it was the very first attempt to utilize an automated market maker model instead of an order book. The idea that had until that moment only been discussed on Vitalik's blog post, was now actively being built (Buterin, 2017). After an initial period of development and bootstrapping, Uniswap started to get traction and received a number of pre-launch grants, including one from the Ethereum community itself, in order for the founder itself and his small team to pursue the effort.

While many of these projects exist uniquely as protocols that run on distributed networks and therefore live in still grey regulatory areas, Uniswap exists both as a decentralized protocol and as a privately held traditional company having legal jurisdiction in the USA and official headquarters in New York. After its launch, Uniswap also raised capital in a number of funding rounds from venture capital firms. These include a one million dollars investment from Coinbase (the largest centralized exchange for cryptocurrencies in the USA) and an eleven million capital raise in June 2020 from among the top venture capital firms in the space as Andreessen Horowitz, Paradigm and ParaFi Capital[3]. As one can infer, for the first three years since its inception in mid 2017, Uniswap had been a founder controlled project which had mostly resembled corporate governance as governance model. In fact, this is also proven by the fact that Uniswap is registered as a for profit organization. For profit organizations need to generate revenue in order to survive. Uniswap's business model is simple and straightforward. For every transaction that occurs on its liquidity pools, the protocol charges a fee of 0.3%.

[2] Retrieved on 12/12/2021 https://defipulse.com
[3] Retrieved on 12/12/2021 https://www.crunchbase.com/organization/uniswap

Of that fee, 0.25% goes to liquidity providers, while the remaining 0.05% goes as company revenue. This obviously means that the higher the volume and number of transactions, the more profitable the protocol is for both liquidity providers and the company.

As the founder wrote in a blog post telling how Uniswap started (Adams, 2019), the protocol was built following blockchain's core values. It is censorship resistant so no actor could stop it. It is decentralized by designed so theoretically no single entity can control it all. It is permissionless by nature as it is built on the Ethereum blockchain so anyone could use it, and finally it is secure as anyone can verify its execution. Nonetheless, the fact that Uniswap also exists as a company having legal jurisdiction, and that there are a set of participants as core developers and investors that own majority of the stake and de facto emulate corporate governance, has raised non negligible controversy in the space and puts into question at least two of the aforementioned points. A company with legal jurisdiction must abide to the rules of such jurisdiction, as a result it is vulnerable to censorship as it may risk legal prosecution. Furthermore, while the protocol runs in distributed fashion, the governance of the protocol itself is not decentralized at all. While this is not necessarily a bad thing, also judging by the growth Uniswap has experienced in the recent past, it certainly goes against the statement that no one singlehandedly controls the protocol.

DeFi summer

As explained above, Uniswap developed as a company having a corporate like governance and running a decentralized protocol. Nonetheless, things started to change in June 2020 when the lending protocol Compound first introduce the idea and launched its governance token COMP. The strength of the concept of a governance token was immediately obvious to every team building DeFi applications, as it introduced three major innovations. First, governance tokens would confer governance rights as: voting on improvement proposals, delegating, proposing and participating in governance forums to each participant owning a token. This proposition felt strongly in line with the ethos of distributed communities as it would theoretically shift power from centralized entities to the community of users, therefore similar to commons that govern common pool resources.

Second, not only these tokens granted governance rights but were also fungible tradeable assets that held value (even if mostly speculative) and were being distributed to the users of the network in order to bootstrap liquidity. In other words, in order for these protocols to incentivize users to deposit liquidity in their smart contracts, they would reward users both with the fees generated by the protocol and with an amount of governance tokens proportional to the liquidity deposited. This mechanisms of incentivizing liquidity deposits by rewarding governance tokens is also known as 'liquidity mining'. Third and final, by allocating a number of governance tokens to themselves, core developers had excogitated a faster and more efficient way of raising capital without having to rely on venture capitalist or crowdfunding.

The combination of community governance, liquidity mining incentives and new source of funding proved to be so powerful that the very vast majority of projects quickly implemented the same idea (although each project with slightly different token distribution and incentive schemes) therefore kick starting the speculative craze later labelled as 'DeFi summer'. However, in the case of Uniswap, the choice of implementing and distributing a governance token was in some ways unnecessary and forced by market conditions. As said earlier, Uniswap already had its own governance structure which was well functioning and most of all guaranteed control and profit to shareholders (core devs and VCs). Also, they had already raised more than ten million dollars though venture capital funding rounds. However, given that most of the other projects were now rewarding liquidity deposits, Uniswap was now facing the risk of seeing its users migrate their liquidity to other protocols that would give them a higher yield. This is at the heart of the 'liquidity battle' between Uniswap and Sushiswap which will be detailed in the next section. As a result of these market conditions, Uniswap finally launched and distributed its UNI token in September 2020 towards the end of Defi summer, clearly more as a business decision rather than a governance one.

While the launch of UNI did function well as a move to both attract liquidity and raise additional funds for the project - the Uniswap treasury today holds around $5 billion USD[4] - it has largely failed in decentralizing governance. As a matter of fact, despite being the biggest decentralized exchange in terms of volume, Uniswap is one of the protocols with the least proposals and community governance development. This might derive from the strong presence of VC participants and by the fact that Uniswap was not originally planned to be governed by the community.

Rules in use

The following subsection will dive deeper into the specific rules that govern and coordinate the Uniswap protocol. As the analysis will cover all the different rule sets as outlined by Ostrom (2005), it will include both the vertical and the horizontal approach to rule analysis.

Position rules

Position rules define the set of possible positions that can be taken as well as the number of participants allowed per position. For Uniswap, at a protocol level the set of positions are:

- Liquidity provider
- Trader (user)
- Governance participant

For each of these positions there is not an explicitly defined number of participants allowed. In theory, the higher the amount of each position the better for both protocol and community. More liquidity providers would imply (but not necessarily) more liquidity in the protocol therefore higher transaction efficiency. More traders would imply higher volume and therefore more fees (revenue) for liquidity providers. Finally, more governance participants would mean a more decentralized governance structure. Moreover, given the permissionless nature of the protocol it is possible for a single participant to occupy multiple positions. For instance, there are core developers and investors which are at the same time liquidity provider, users of the network and obviously governance participants. At the same time, VCs which invested in the project in early stages were rewarded with both company equity and governance tokens. Venture capital firms, Andreessen Horowitz in particualr, are among the largest UNI token holders. The next section will detail what are the necessary actions to be taken to occupy the listed positions.

Boundary rules

Again, the ethos of decentralized protocols is to make them available to anyone with low entry barriers. As a result, literally anyone can trade on Uniswap and anyone can provide liquidity to one or multiple pools. In order to trade, all one has to do is to download a browser wallet like Metamask[5] and be in possession of even a single cryptocurrency. The wallet will interact with the smart contracts of Uniswap and allow one to

[4]Retrieved on 12/12/2021 https://dune.xyz
[5]https://metamask.io

exchange one token for the other without ever having to give up the custody of own funds. As described in the previous chapter this goes in strike contrast with centralized exchanges where one first has to transfer funds to their platform for then being able to trade. The same process just described goes for providing liquidity into a pool. No 'Know Your Customer' due diligence is required nor any credit score. Just the proof of funds in ones wallet.

As for becoming a governance participant, the process is slightly more articulated. The very first step is to own UNI tokens. This can be achieved either by buying it from the market or by receiving it as a reward from providing liquidity to one or multiple pools. However, simply owning UNI tokens is not enough. In order to participate in governance by, say voting, one must first delegate the tokens, and therefore voting power, to an address. This address can be ones own address or one from a user which one trusts or believes in.

Furthermore, Uniswap implements a risk mitigation process in order to avoid users will large amount of capital to buy UNI token and immediately use them for voting on a given proposal. In order for one to vote on a proposal, one must have delegated their voting rights before the start of the voting process and even before proposal submission.

Choice rules

Choice rules are simple and straightforward. Traders can decide to either buy or sell. Liquidity providers can choose whether to deposit or withdraw liquidity in case they have already deposited and perhaps accumulated yield. Finally, governance participants can decide whether to vote on proposals, usually votes are 'for' or 'against', they can choose to delegate their votes and finally, in the case they have enough tokens, they can decide to create and submit a proposal.

Aggregation rules

As for aggregation rules, the initial parameters set by Uniswap core developers were the following. In order for one to create a proposal to be voted for, one must have at least 1% of the total UNI supply, equivalent to 10 million UNI tokens. Important to note that proposals not only come in the form of posts in the governance portal, but are also executable code that get implemented in the smart contract in case the proposal passes. In order for the proposal to pass, it must achieve a quorum of 4% of the total UNI supply, 40 million UNI tokens. Arguably, the quorum was said to set to be this high to ensure that only the proposals with high participation would pass. Furthermore, once a proposal is submitted, participants have a seven day voting period. To conclude, in the eventuality that a proposal passes, before being implemented it is required to sit in a Timelock for a minimum of two days. This means that for two days minimum the code itself cannot be implemented nor modified, this in order for the core team to audit it and spot potential flaws.

Information rules

For Uniswap, as for most of the blockchain communities that live online, the main channel of communication is the Discord application. Discord is a voice over internet protocol (VoIP) applications which is utilized for communicating through calls, video calls and text messaging. One of the reasons why it became so popular is because it is quite flexible for organizing chat rooms. Figure 5.5 below is a snapshot of Uniswap's community room. On the left hand side one finds listed all the channels covering different topics one might want to discuss. From the announcement channel, to general conversations regarding the project, to channels exclusively for developers and technical troubleshooting. As the snapshot taken could not cover all of the different channels, Figure 5.5 on the right hand side displays an additional snapshot taken of the governance channels of Uniswap - where the community can discuss about governance proposals and implementations - as well as channels created exclusively for users of diverse nationalities. As one can observe, there are all sort of languages included from Chinese to Indonesian and even Arabic. This also gives a sense of the globalization and decentralization of these communities.

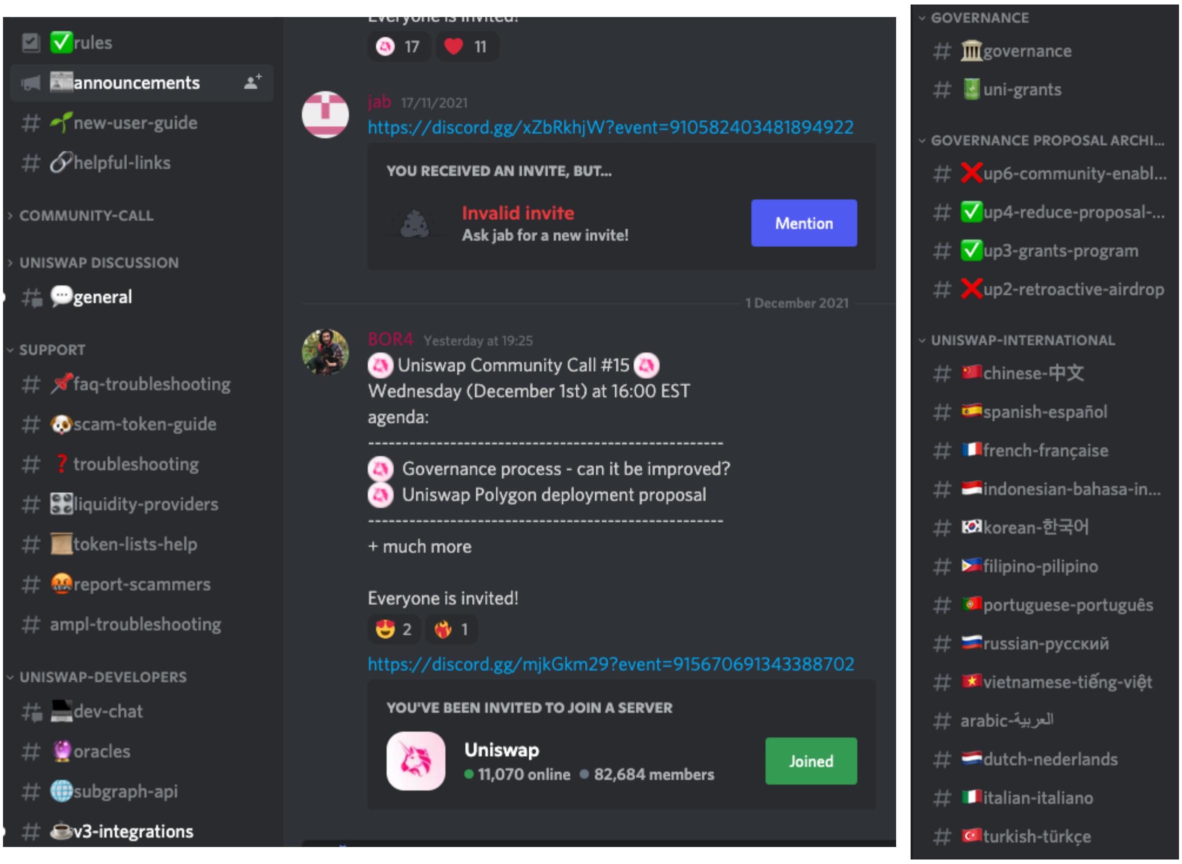

Figure 5.5: On the left: Uniswap discord server with all main channels. On the right: Uniswap channels covering governance proposals and different language channels.

Nonetheless, other than Discord where users can communicate and exchange information at an informal level, when it comes to actually proposing changes to the protocol or to its governance, Uniswap has set a specific information flow. Given that casting votes on a blockchains comes at a cost since each vote has to be recorded on the public ledger (therefore mined in exchange for a transaction fee) it would be quite inefficient to vote for each proposal 'on-chain', also considering that quorum could potentially not be reached and therefore the voting process has to be repeated again, incurring in more transaction costs. To solve this problem, Uniswap developed a multi layered proposal discussion process where only proposals that are guaranteed to reach a minimum quorum are allowed to officially be voted for on-chain. The following paragraph will discuss such process as well as the relative platforms utilized for each step of the process.

The first step is defined as 'Temperature Check'. In this stage, if a user desires to make a proposal, all he has to do is access the Uniswap forum [6] and ask an unbiased question, in the form of a post, about a potential change. The idea here is to determine whether there is sufficient will to make changes to the status quo. The community will then use the Snapshot portal [7] to indicate their interest in bringing the proposal to the next

[6] Retrieved on 13/08/2021 gov.uniswap.org
[7] Retrieved on 13/08/2021

stage. After a three day voting period, if the proposal has reached a majority vote with at least 25 thousand votes then it can proceed.

The second step is defined as 'Consensus Check' and its goal is to establish a formal discussion around a potential proposal. The same user, or set of users, which posted the 'Temperature Check' proposal should now submit a new proposal to the same Uniswap forum, this time with a voting period of five days. This stage aims at making community participants discuss more deeply and critically on changes being proposed with relative impartiality. For a proposal to pass this stage it should reach a quorum of 50 thousand yes votes.

After a certain proposal has passed both the temperature and the consensus check, the third and final step is the actual 'Governance proposal'. This step requires the proposer to actually write the code for protocol upgrade, which can be voted for on the Governance portal. Every written code has to be audited by a professional auditor and the process is reimbursed by the community treasury. On top of this, the proposer has to make sure at least 2.5 million UNI tokens are delegated to his address in order for him to submit the proposal officially 'on-chain'. This final voting process takes 7 days and if the proposal where to pass then a two day time lock follows before deploying the code. The two day time lock is utilized in order to check the code once more in order to look for vulnerabilities.

Payoff rules

Ostrom (2005) defined payoff rules as external rewards or sanctions applied to given actions that different participants can take. In the case of Uniswap, Liquidity providers are the only set of participants that are subject these types of rules. In particular, liquidity providers are rewarded with a percentage of the fees generated by the pool in exchange for the liquidity provided. There are three different fee tiers a pool can be subject to, being 0.05%, 0.3% and 1%. The fee tier is decided upon by the community and varies depending on the liquidity a certain pool has. The higher the fee the 'payoff' for liquidity providers depositing in that pool.

Scope rules

Scope rules are the ones that must or must not affect known outcome variables as a result of actions taken in the action situation. As mentioned earlier, given the particular setting on which the community interacts, there are no strict rules but only options for different participant that lead to different outcomes. As a result, in this regard, most of the rules can be also seen as scope rules. For instance, the payoff rule discussed just above, aims at incentivizing liquidity providers to deposit liquidity in the pools, therefore its 'scope' is to increase the overall total value locked of the protocol. Another example is in regards to the voting mechanism. In order for a participant to vote on a certain proposal, he must delegate his UNI token (voting power) before the proposal has even began to be discussed in the forum. This security mechanism avoids wealthy individuals from simply buying large quantity of tokens at will at any time for the simple purpose of manipulating voting processes. As a result, this can also be categorized as a scope rules as its 'scope' is to aid and guarantee a healthy community involvement.

Evaluative criteria

The following section will go through the different metrics utilized to assess the performance of the protocol and will also investigate on the impact certain rules may have on the outcomes. The analysis will be conducted by cross evaluating the data from three different blockchain analytics platform namely, Dune, Tally and Sybil[8].

[8] https://dune.xyz, https://sybil.org, https://www.withtally.com

Total value locked & volume

As visible from Figure 5.6, the total value locked in Uniswap had quite a growth since inception. Launched in November 2018, by February 2019 it had already locked around one million dollars. Exactly one year later, the TVL had grown 30 fold to 30 million dollars. Not only such an increase is incredible for any type of business, but it was also achieved during a period of bear market conditions. Meaning, there was little if no speculation and the very majority of users depositing liquidity into the protocol were early adopters with a very high degree of conviction. The 2019 TVL increase can arguably be regarded as an organic growth with limited speculation, which aided to a sustainable development of an early stage protocol that would experience a massive inflow of users and capital shortly after. This is generally true for most DeFi applications. Until early to mid 2020, decentralized finance applications were mostly regarded as experimental project that would take years to refine and reach substantial adoption. While the former might certainly be true, the latter was proven not so precise.

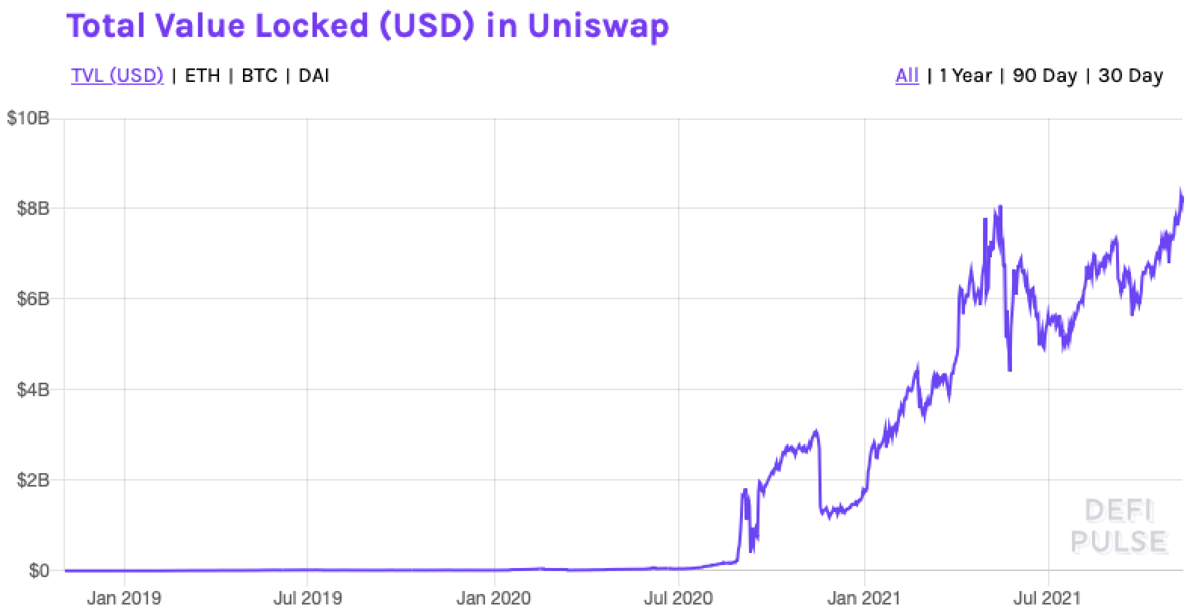

Figure 5.6: Total value locked in the Uniswap protocol from launch to January 2022 (source: `https://www.defipulse.com`)

As introduced above, 2020 was the year where DeFi applications started to gain more and more attention given their proven resilience and attractive yields. The TVL of Uniswap had quite a regular growth for the first half of 2020 and well into DeFi summer. However, everything drastically changed when Uniswap introduced UNI as additional yield for liquidity providers. As clearly visible in the figure above, the total value locked increased from 170 million to north of 3 billion dollars in the span of two and a half months. This is a clear example of how payoff rules can greatly influence the performance of a protocol. Moreover, one can also clearly see how the TVL decreased sharply after the first initial peak, this was due to the fact that initially UNI incentives had been planned for a period of two months. Once the rewarding period was over, liquidity providers were extremely quick to move their funds to higher yielding platforms. This behaviour highlights two major points. The first one is that the exit costs from these protocols is extremely low, in fact one can see the ease and speed at which liquid capital moves from one smart contract to the other. The second is a demonstration on how speculative these markets can be. The examples just described above show how, regardless of governance and protocol innovation, a great deal of users will interact with decentralized exchanges mostly for chasing returns on their capital. While this might be optimal for bootstrapping liquidity it might not be the most optimal for innovation.

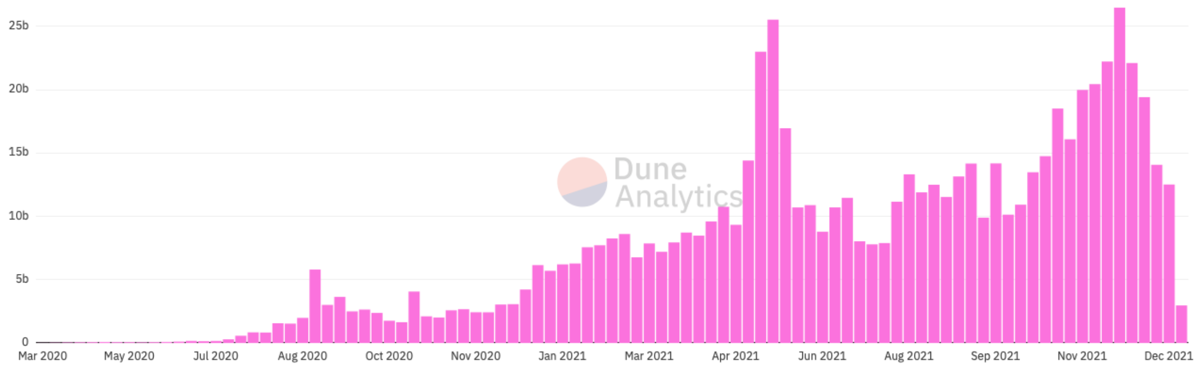

Figure 5.7: Weekly Uniswap volume since March 2020

Finally, as already visible in Figure 5.4, the volume of Uniswap is by far the largest in the entire DeFi ecosystem, and is in fact many multiples larger than its direct competitor, Sushiswap, on a weekly basis. As a result, Uniswap has been among the protocols that have guaranteed the most returns for liquidity providers. Figure 5.7 above highlights as well how substantial trading activity only really picked up around mid 2020, actually before the release of the UNI token. Nonetheless, trading activity has increased quasi consistently since the initial UNI distribution. In particular, May and September 2021 presented weeks where volume even surpassed $25 billion USD in a week.

Community size

As one could infer, an increase in TVL normally also translates into an increase of users. However, by comparing the TVL and user growth graphs one can notice that TVL had a much steeper growth. This means that, while the amount of users did grow, the average deposit amount grew even quicker. Nonetheless, user growth was also quite surprising. In January 2019, few months after launch Uniswap was counting around merely 200 users. By the end of the year, user count was around 24000. One important thing to point out is that, 24 thousand addresses does not exactly equate to 24 thousand individuals. In fact, one individual can utilize multiple addresses. This is particularly true for users with large amounts of capital or users really concerned with security. Nonetheless, the growth is non negligible. Furthermore, one can see that, as TVL, user count started picking up considerably right after the announcement of liquidity mining, and in a short span of time user count increased five fold to half a million users.

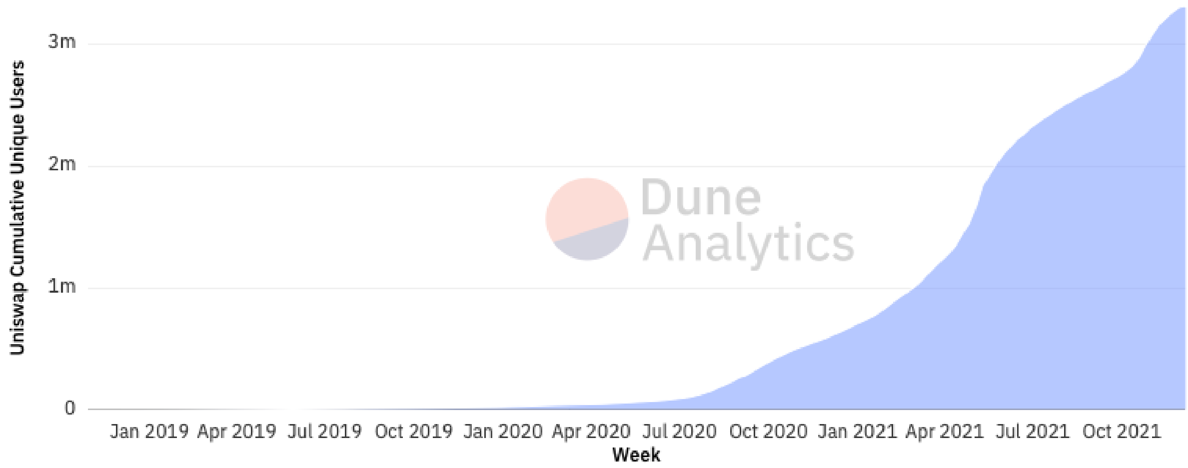

Figure 5.8: Uniswap protocol users since inception

One can also notice that while user TVL has decreased in mid 2021, given the momentary burst of the hype of the first half of 2021, user count never stopped rising, reaching today more than three million users. Again, a five fold increase in around 8 months. This is a strong sign of adoption even if capital deposited has not risen in parallel. To conclude, another interesting data point is the overlap between traders and liquidity providers, meaning how many of the former also form part of the latter cluster. As visible in Figure 5.9, thus far only 11.6% of users that have ever traded on Uniswap are also providing liquidity to one of the pools. This analysis comes in handy to understand that these two sets of participants, namely traders and liquidity providers, are pretty much separate sets of individuals.

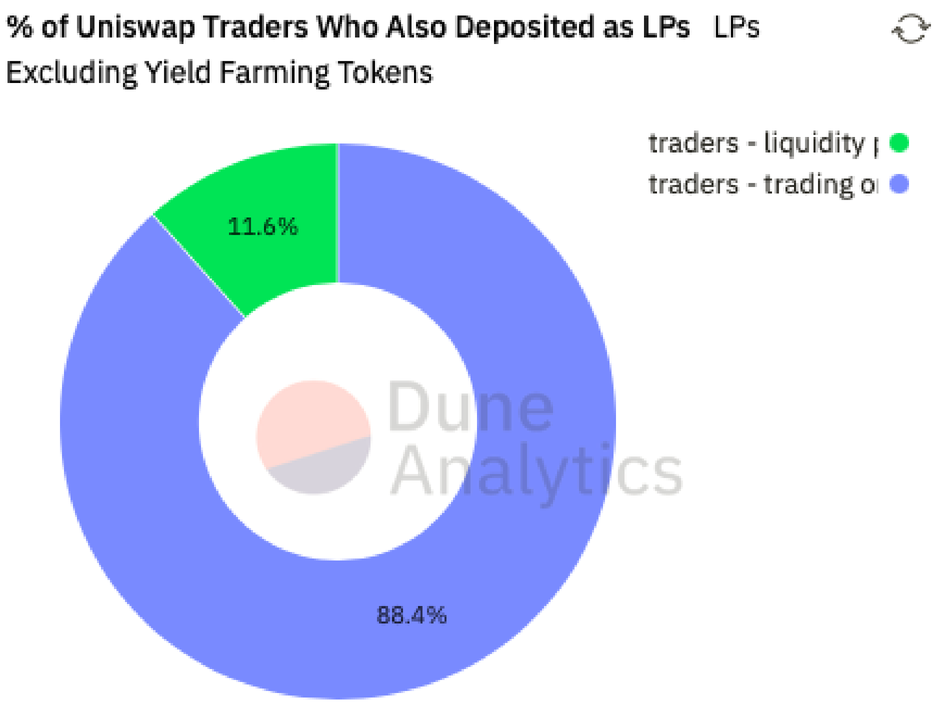

Figure 5.9: Uniswap percentage of traders that are also liquidity providers

Community involvement

Community involvement is one of the most insightful metrics to be analyzed, also because its method of analysis differs for every different project. For Uniswap there are a number of different ways in which one can measure involvement. The first one is to figure how many UNI tokens - of the ones in circulation - have been delegated and therefore able to vote. At the time of writing there are 627,929,159 UNI tokens in circulation[9]. On the other hand, from the data retrieved from Dune and displayed below in Figure 5.10 one can see that the total amount of UNI delegated accounts to 200,962,736 tokens. This means that only 32% of the tokens in circulation are set to participate in governance.

Figure 5.10: From left to right: (i) total number of UNI tokens that have been delegated (therefore able to vote), (ii) total number of addresses that hold voting power, (iii) total number of addresses that hold UNI tokens

The other two data point presented in Figure 5.10 display respectively the total number of addresses that hold voting power and the total number of addresses that hold UNI tokens. This shows that of all addresses holding UNI tokens, only 2,9% have tokens delegated and therefore have voting power. This data point can be telling in different aspects. On one side, it shows how communities will naturally tend to some sort of representative democracy by delegating their voting power to individuals they believe are better prepared to take decisions. On the other, it also underlines centralization of power in the hands of a few. Overall, what the three data points in Figure 5.10 highlight is that: over two thirds of the individuals owning UNI do not hold it for governance purposes, and that voting power is concentrated in a mere fraction of existing addresses.

Furthermore, Figure 5.11 below given a visual representation of the total amount of UNI tokens delegated over time. As noticeable, since inception in October 2020, the amount of tokens delegated grew quickly over 50 million. These are attributed to the tokens held by core team and early VC investors. After this initial steep delegation growth, delegated UNI has grown discretely until June of 2021 from where delegation has mostly plateaued. The sudden decrease and increase in tokens delegated that occurred a little before April 2021 can be explained by a large address (or group of addresses) that undelegated to an address just to delegate again to someone else.

[9]https://www.coingecko.com

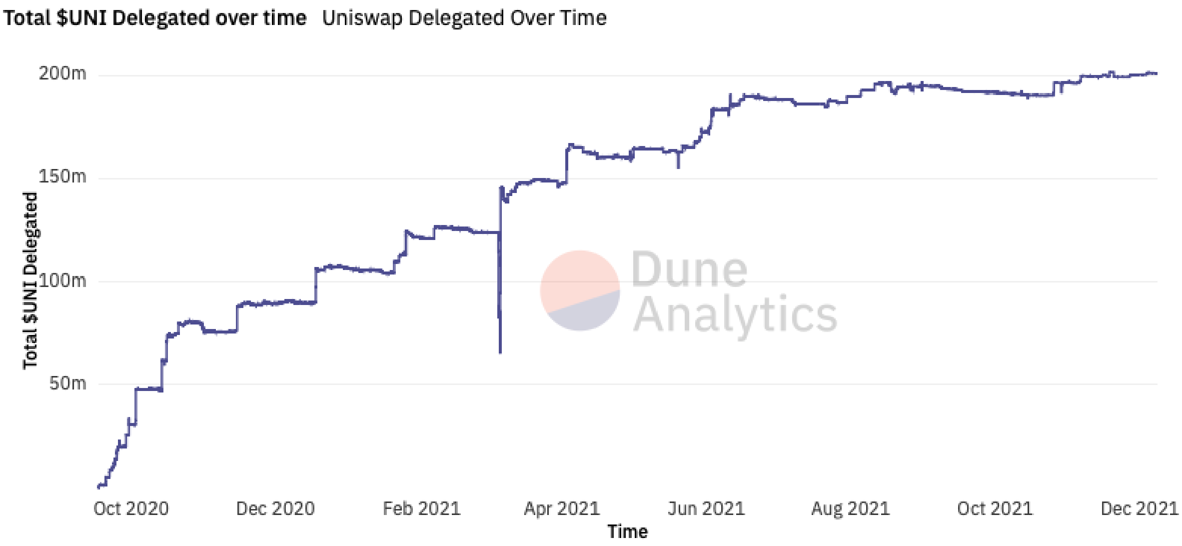

Figure 5.11: Cumulative amount of UNI tokens delegated over time

Another way in which one can gauge community involvement is by looking at the relative amount of proposals the community has voted for. Moreover, given that voting occurs on chain, one can also inspect the voting process itself and retrieve valuable information from it. Figure 5.12 below, provides a visual overview of all the proposals that have been voted for so far. Until this moment in time, only nine proposals have made it through both the temperature and the consensus check. Of the nine, five have passed, three have not reached the quorum of 40 million 'for' votes, and one proposal was cancelled.

Proposal	Votes for	Votes against	Total votes
Add 1 Basis Point Fee Tier EXECUTED · ID: 9	71.37M	0	71.37M 41 addresses
Upgrade Governance Contract to Compound's Governor Bravo EXECUTED · ID: 8	63.46M	2.43K	63.46M 101 addresses
Community-Enabled Analytics CANCELED · ID: 7	47.62M	46.99M	94.61M 121 addresses
DeFi Education Fund EXECUTED · ID: 6	79.68M	15.04M	94.72M 296 addresses
DeFi Education Fund QUORUM NOT REACHED · ID: 5	14.46M	5.65K	14.47M 55 addresses
Reduce the UNI proposal submission threshold to 2.5M EXECUTED · ID: 4	90.98M	2.04K	90.98M 148 addresses
Uniswap Grants Program v0.1 EXECUTED · ID: 3	60.09M	9.3K	60.1M 189 addresses
Retroactive Proxy Contract Airdrop — Phase One QUORUM NOT REACHED · ID: 2	37.56M	1.28M	38.84M 340 addresses
Reduce UNI Governance Proposal & Quorum Thresholds QUORUM NOT REACHED · ID: 1	39.6M	696.86K	40.29M 320 addresses

Figure 5.12: List of proposals that have so far been voted for on Uniswap (source: `https://www.withtally.com`)

By comparing this data to the one presented for community involvement, one can notice that in none of the proposals the total amount of delegated UNI participated in the voting. As a matter of fact, in the last five proposals that have taken place from June 2021 onward, not even half of the delegated UNI participated. What is also striking is the amount of voting power that is held by a small number of addressed. For instance, in the very last proposal 'Add 1 Basis Point Fee Tier' one can see that only 41 addresses cast 71 million votes. In numbers, 0,4% of address delegates possess 35,5% of the voting power.

Nonetheless, in some cases delegates with large voting power have also voted in favor of proposals that could benefit the community at large. A good example was the proposal for reducing the proposal submission threshold which was initially set at 10 million UNI token, or 1% of the total supply. At current market prices, this would mean that a governance participant would have had to accumulate nearly $170 million worth of UNI token in order to just submit a proposal for vote. This obviously goes in stark contrast with the ethos of decentralization portrayed by the projects in the space as there are very few participants which dispose of so much wealth. As a result, a proposal was passed to reduce the submission proposal threshold by 75% to 2.5 million UNI tokens. While this still represents a large dollar value, it should make it easier for smaller holders to unify their voting power under one delegate in order to submit proposals. As visible in Figure 5.13, the proposal passed with nearly 100% of 'for' votes and a participation rate of almost 50%. What is noticeable as well is that also the largest holders, being venture capital fund 'a16z' and universities as 'Harvard Law Blockchain', 'MIT bitcoin club' and 'Stanford Blockchain Club', voted in favour.

The voting distribution presented below in Figure 5.13 also provides another insight unrelated to the voting mechanism itself. As detailed above, a number of wallets containing large amounts of tokens belong to the most prestigious universities in the world. But what is more interesting is that they belong to faculties ranging from law (Harvard) to engineering schools (MIT). This means that the innovation being brought forward is not only technological but encompasses a variety of other fields of study as well.

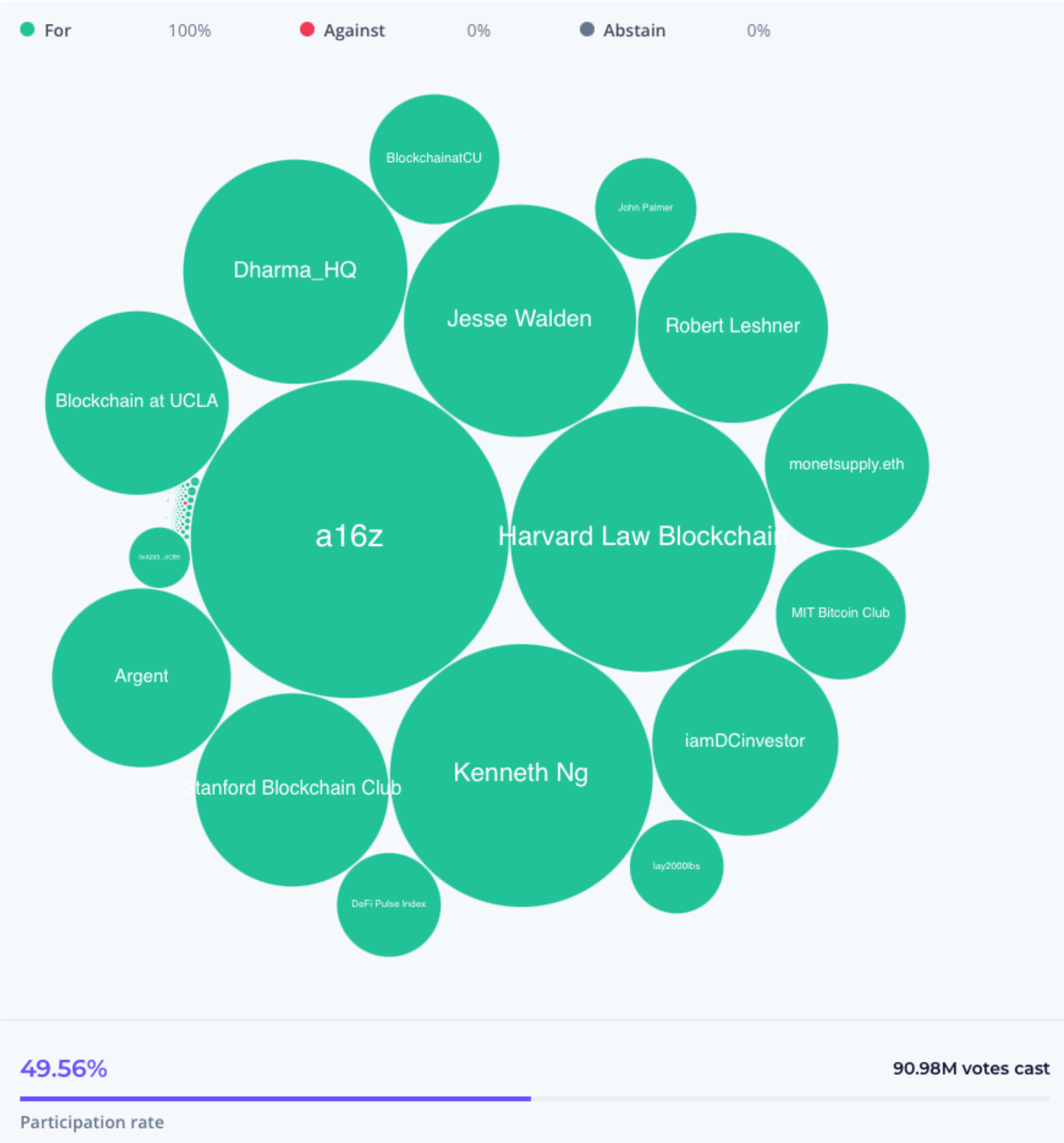

Figure 5.13: Vote distribution for reduction of UNI proposal submission threshold (source: `https://www.withtally.com`)

Token distribution

Given the one token one vote system implemented by Uniswap, token distribution among participants is a crucial metric to determine whether voting power is actually decentralized as it is intended to be or not. A first impression is given by the initial (genesis) token allocation decided by the core developers team in October 2020 and presented below in Figure 5.14. It might be useful to remember that until the token release the project was totally controlled and decided upon by the core council of developers and early investors. By distributing governance tokens the team claimed it was handing over governance power to the community and as a result Uniswap would 'officially be a publicly owned and self-sustainable infrastructure while continuing to carefully protect its indestructible and autonomous qualities' (Uniswap, 2020).

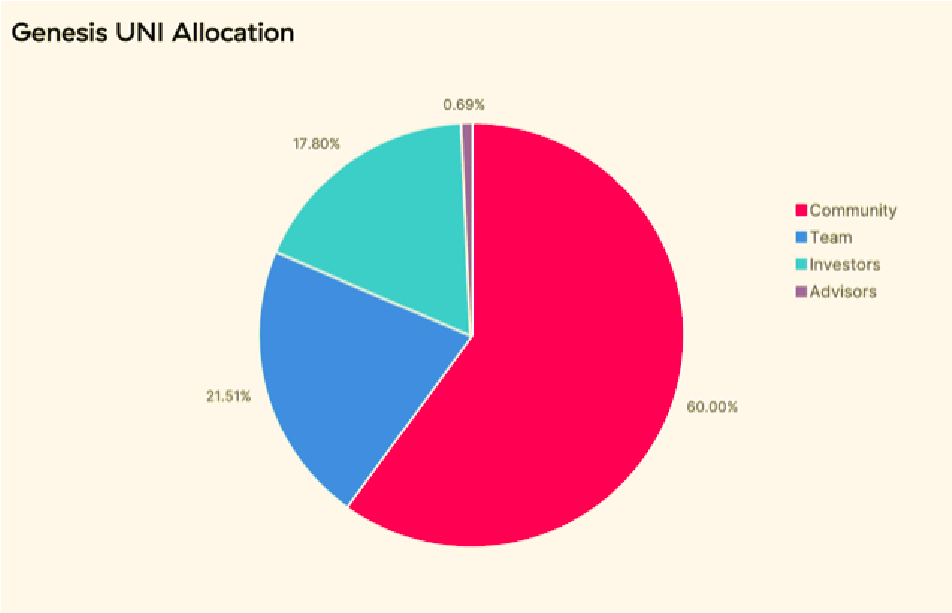

Figure 5.14: Uni token initial distribution Eichholz (2020)

Uniswap therefore minted (created) 1 billion UNI tokens to be distributed in 4 years as follows:

- 60% to community members
- 21.266% to team members and future employees
- 18.044% to investors with 4 year vesting period
- 00,69% to advisors with the same 4 year vesting period as presented below in Figure 5.15

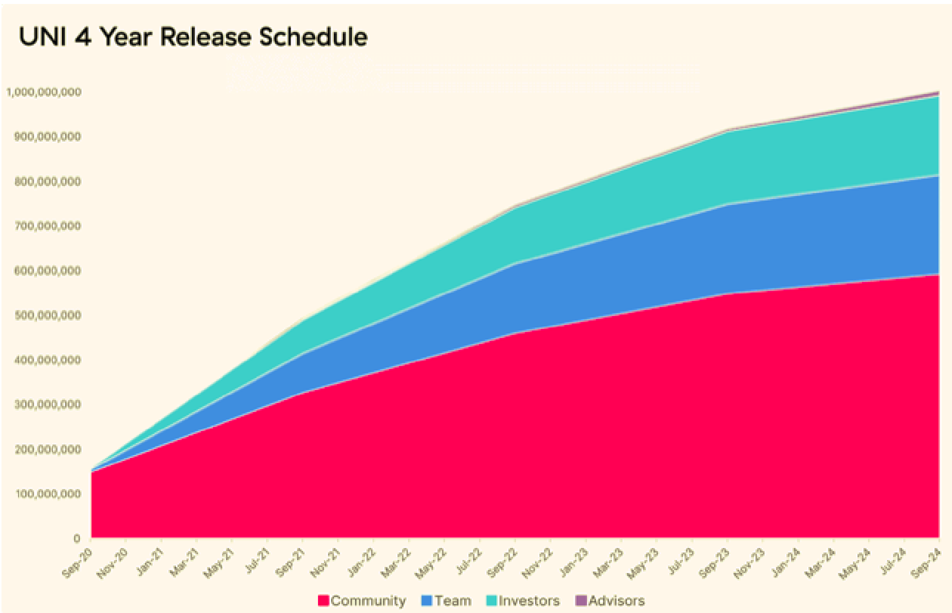

Figure 5.15: Uni token release schedule (Eichholz, 2020)

As noticeable, even though more than 50% of the tokens were planned to be distributed to the community itself, around 40% of them were distributed to developers and early investors. While this may not necessarily be something bad for the development of the project given that its decision making is still in the hands of stakeholders which really have at heart its progress, it certainly does not represent the much advocated governance decentralization.

As of today, nearly one year after the initial token allocation, voting power distribution is still heavily centralized. Thanks to front end platforms like Tally, one can see both the amount of tokens held by certain wallets as well as who owns these wallets. A list of the ten largest UNI token delegates is provided below in Figure 5.16. By doing some data analytics one would find out that, the first 10 holders cumulatively hold 92.86 million votes, or the equivalent to 46% of the total voting power. The first 25 holders cumulatively hold 80% of the voting power (161.58 million votes) while the first 50 holders cumulatively hold 98% (197.58 million votes) of the total voting power. As visible, this stands far from any sort of democratic decentralized governance and is more a resemblance of a digital plutocracy.

Voter		Proposals voted	Total votes
1	a16z	6	15M
2	0xe024...26bF	0	12.8M
3	Autonomous Proposal: Uniswap Grants Program v0.1 (Passed)	1	9.8M
4	0x8E4E...a42E	1	9M
5	Harvard Law Blockchain	3	8.61M
6	Kenneth Ng	5	8.15M
7	Jesse Walden	3	8M
8	Dharma_HQ	5	7.46M
9	0xF977...aceC	0	7.23M
10	cUNI Multisig	1	7.11M

Figure 5.16: List of ten largest Uniswap token delegates (source: `https://www.withtally.com`)

One such instance of clear plutocracy occurred during the very first Uniswap governance proposal dating October 12, 2020. At the time there were less tokens in circulation, so the once distributed to early investors had even a higher weight during voting. The proposal was made by a company involved in the development of digital assets called Dharma Capital. In one single proposal, Dharma propose to lower both quorum and proposal submission threshold. Respectively, from 4% to 3% of total supply (30 million UNI) and from 1% to 0,3% of total supply (3 million UNI). While the proposal might have appeared legitimate given the high initially thresholds, in reality it was a early move from Dharma to try to take total control of the protocol governance given that, by joining forces with another large wallet of almost 15 million tokens they could have singlehandedly submitted and voted for proposals reaching quorum and majority by themselves. Figure 5.17 gives a visual representation of the voting results for this proposal. Fortunately enough, they did not reach the quorum of 40 million votes by just 3 million votes. Also, the fact that a participant proposed two governance changes in one single governance proposal is a clear signal of the earliness of DAO governance and that many more design iterations will be needed during the years.

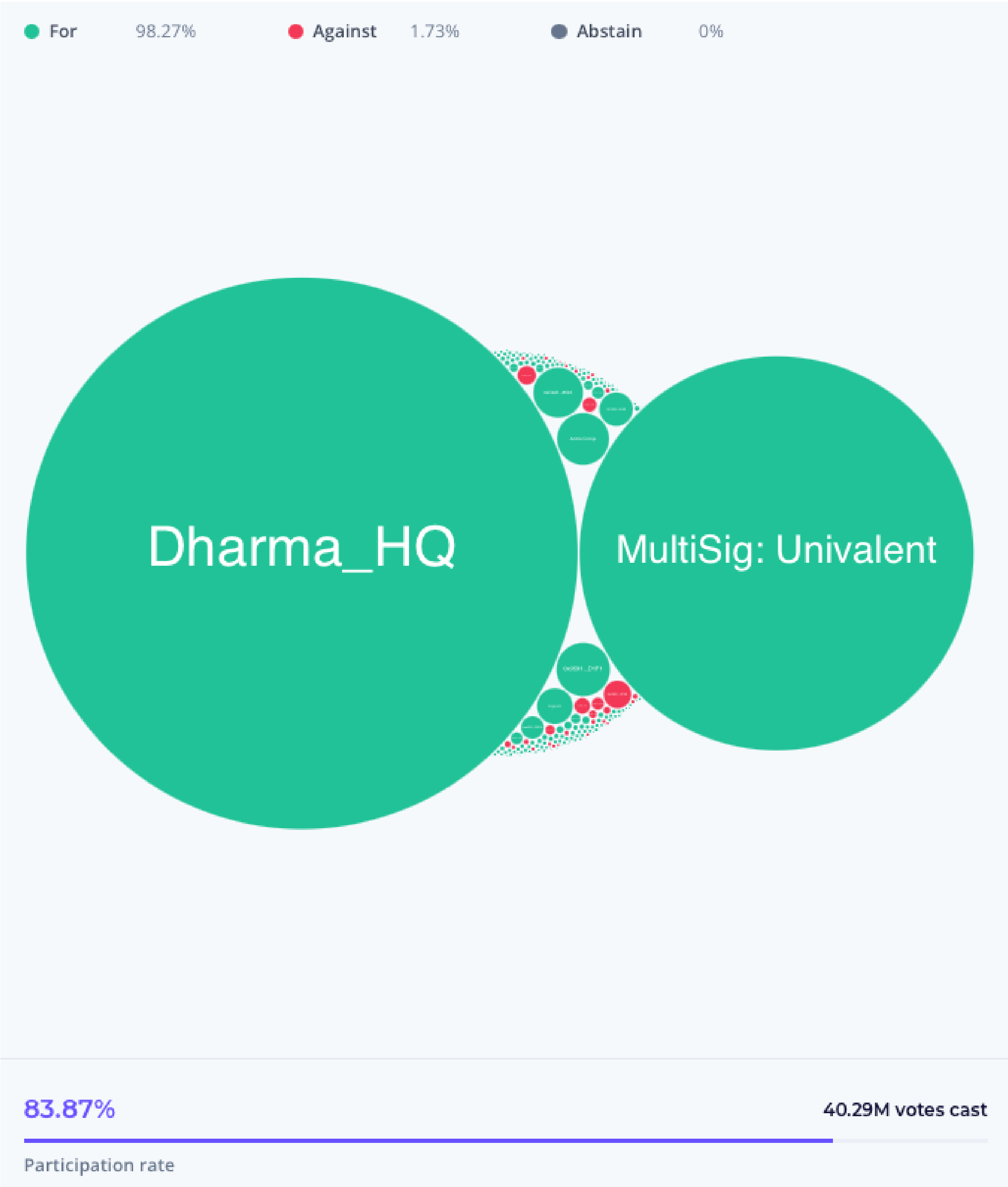

Figure 5.17: Uniswap voting distribution for first governance proposal on changing quorum threshold (source: `https://www.withtally.com`)

5.5. Sushiswap

One of the features of open source technology is the possibility to literally copy the source code of other projects and re-deploy them by adding or subtracting any additional specific at will, if any. In the blockchain space, the process of iterative development that follows the copying of source codes is known as 'forking'. Sushiswap launched in September of 2020 as a fork of Uniswap. Until that moment in time, Uniswap had been one of the most successful DeFi applications having the highest TVL and trading volume. However, during the whole of DeFi summer Uniswap did not launch any governance token both because it already had an internal and legal governance structure, and because the protocol was attracting so much liquidity and users that the Uniswap core team did not feel the need to distribute further incentives in order to attract liquidity.

This of course presented an opportunity for savvy developers to fork the already successful Uniswap protocol implementation and add additional economic rewards on top of it in order to incentivize users providing liquidity on Uniswap to migrate their liquidity to the now more profitable Sushiswap liquidity pools. This is also known as 'vampire attack'. In their very first post (Nomi, 2020), the Sushi team claimed that Sushiswap was an 'evolution' of Uniswap, by 'taking Uniswap's elegant core design and adding community oriented features that improved the design of the protocol and provided further benefits for the actors involved'.

As will be shown in the evaluative criteria section, in a very first instance Sushiswap did manage to 'steal' liquidity from Uniswap and therefore bootstrap its own liquidity for a successful launch of Sushiswap. Also worth mentioning that unlike Uniswap, the core team of Sushi was completely anonymous for the general public. Nonetheless, a large amount of users still trusted the team and deposited their funds in Sushi's smart contracts. Being a community oriented and driven project from the start, Sushi also implemented different governance mechanisms which will be discussed in the following sections. Finally, perhaps one of the main differences between Sushi and Uniswap is that, at least at the initial stages, no funding was received from the team from venture capital firms. As a result, the core team of developers were the sole decision makers of the protocol.

Rules in use

Position rules

As for Uniswap, and all of the projects analyzed in this thesis, the three different set of positions participants can take at a protocol level are: liquidity providers, traders and governance participants. For each position there is not a limit to the amount of participants that can occupy that position and a single user can also occupy two or more positions at once. As a matter of fact, every core developer of Sushi occupies all three positions.

Boundary rules

Boundary rules are the first set of rules where Sushi differs from Uniswap. As for becoming a trader or a liquidity provider there are basically no entry barriers. All users have to do is interact with liquidity pools in order to transact or deposit liquidity respectively. However, in order to become a governance participant and effectively participate in proposal submission and voting, holding Sushi tokens is not sufficient. Contrary to Uniswap where one UNI token granted one vote, for Sushi in order to cast one vote one must hold one 'sushipowah' token. In order to obtain sushipowah tokens, sushi holders have two different alternatives. The first one is to deposit liquidity into the SUSHI-ETH liquidity pool. For each sushi deposited, liquidity providers would receive two sushipowah tokens. The second option is to deposit sushi into the 'sushibar' smart contract and receive xSushi tokens in exchange. For each xSushi token users would receive one Sushipowah token. The purpose of the sushibar will be explained in the payoff rules section. These particular boundary rules for users to become governance participants highlight how in the case of Sushiswap, it is not enough to simply hold Sushi tokens, but users must first put their tokens at stake. The choice of this particular mechanism is quite ingenious because it implies that for users to participate in governance they must first put their working capital at risk. As a result, this should suggest that users who participate in governance are actually believers of the project and are interested in its longevity. Also, adding this extra step of depositing sushi in either mentioned liquidity pool or in the sushibar in order to obtain sushipowah is an additional security layer that prevents malicious users from simply borrowing sushi tokens from other protocols and using them directly for voting.

Choice rules

The list of choices users have when participating in governance are no different from the other protocols. Users can choose to vote against, for or to abstain from any given voting process. Also, users can choose to propose changes either to the governance itself or to the operations of the protocol by submitting proposals through the governance forum. Another important fact to mention is that the Sushi team has explicitly distinguished the type of proposals that the community can vote on from the ones that are decided upon exclusively by the core team of developers. On one side, the community at large can vote for major structural changes to the protocol and on how to deploy the capital in Sushi's treasury. On the other, smaller changes regarding the operations of the protocol and the implementation of additional trading pairs are decided upon by the core team.

Aggregation rules

Aggregation rules are quite simple and straightforward. For proposals that need to be passed and voted by the community, majority and a quorum of 5 million Sushipowah need to be reached in order for the proposal to pass. While for the operational changes that are voted by the core developers, at least 6 out of the 9 members need to agree for changes to be approved.

Information rules

Differently than Uniswap, Sushi does not have a multi tier system for participants to discuss on proposals and then finally vote on the governance portal. The main communication channel still remains Discord given its ease in creating separate chat rooms for different topics. As for discussing governance and protocol changes and finally voting on them, Sushi uses two different platforms. The first one is the regular discussion forum, as displayed below in figure Figure 5.18. After identifying on the forum which proposals are the community mostly interested in, then voting occurs on the Snapshot platform (off-chain). Interesting to note that while Uniswap uses Snapshot as an off-chain platform for the temperature and consensus check process, Sushiswap utilizes the same platform as a final and settling voting venue. However, since votes are not cast directly on the blockchain it is not possible to perfectly track the voting process as with Uniswap.

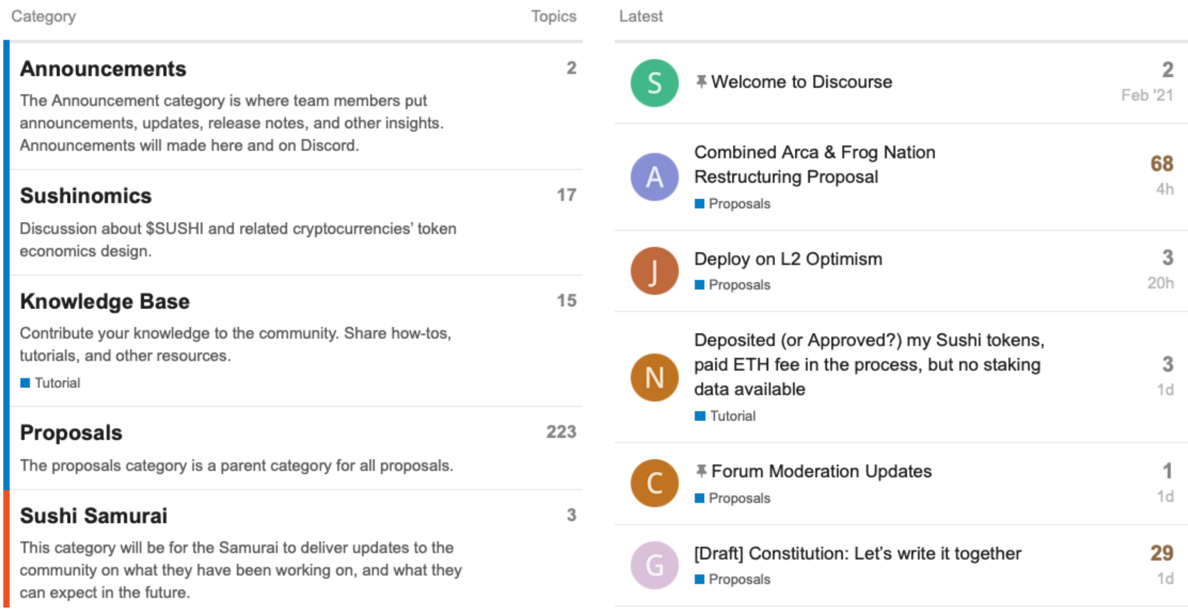

Figure 5.18: Snapshot of Sushiswap's forum main page (source: `https://forum.sushi.com`)

Payoff rules

Payoff rules are perhaps the second set of rules that mostly mark a difference between the Uniswap and Sushiswap protocols. Sushiswap also charges an 0,3% fee for users to trade in the liquidity pool. However, of that fee, only 0,25% actually goes to liquidity providers, while the remaining 0,05% goes to xSushi holders. Or in other words, to users that have deposited sushi tokens in the sushibar smart contract in exchange for xSushi tokens. This is arguably the major difference between Uni and Sushi tokens, that while the former can be only utilized for voting purposes, the latter can be utilized in a value accrual mechanism therefore giving Sushi holders not only the rights to participate in governance, but also a claim on part of the revenue generated by the protocol. As explained above, the Sushi team developed a more secure mechanism for users to obtain voting right through depositing their tokens either in a liquidity pool or in the sushibar. Therefore, since depositing sushi in the liquidity pool grants providers a portion of the fees, the team had to find a way to incentivize users to also deposit sushi in the sushibar, otherwise all sushi token would have been staked in the liquidity pool given higher incentives.

Scope rules

As in the case of most projects in the space a number of rules occupy more than one category in Ostrom (2005) rule classification system. For instance, the boundary rules presented above also function as scope rules, since the scope of making users deposit Sushi tokens into the Sushibar, in exchange for sushipowah, is to guarantee the commitment of governance participants. On the other hand, the fact that depositing sushi into the Sushi-Eth pool grants twice the voting power per sushi with respect to simply depositing sushi in the sushibar, also has the scope of making the Sushi-Eth pair more liquid and therefore more trading efficient. Additionally, providing liquidity to the Sushi-Eth pool would also expose providers to impermanent loss, this also explains the granted voting premium. Finally, payoff rules are also a strong example of rules that also belong to the scope rules section. As a matter of fact, depositing sushi into the sushibar is rewarded with 0,05% of the total fees generated by the protocol in order to incentivize users to deposit their sushi in that specific smart contract. In other words, the scope of that 0,05% reward is to incentivize governance participation.

Evaluative criteria

Total value locked and volume

Tracking the TVL of both Uniswap and Sushiswap protocols can allow one to notice exactly the date and the impacts of the vampire attack that Sushi had on Uniswap. As noticeable, from Figure 5.19 and Figure 5.20 below, the very first attack occurred in mid September of 2020 when Sushiswap had just launched. One can perfectly see how on the same date, the TVL of Sushiswap increased by slightly more than $1 billion and the TVL of UNI decreased by nearly the same amount. Nonetheless, as soon as the incentives on Sushi ran out, liquidity quickly moved back to Uniswap and other protocols that were launching at the time.

Furthermore, one can notice from the TVL graph of Uniswap that its TVL increased continuously from mid September until mid November. This period also corresponded to the launching period of their own token UNI. However, in mid November, the Sushi team launched a second vampire attack by increasing considerably the rewards on their own protocol. As visible in the charts below, a sudden decrease in Uniswap TVL corresponded to a simultaneous increase in Sushiswap TVL. Nonetheless, from that point on both protocols started to grow at similar pace given that the technology had matured enough and more and more users were flowing into the space using both protocols. To date, both protocols have grown considerably and in slight different directions. While Uniswap has continuously tried to increase the amount of token pairs offered as well as more efficient liquidity pools, Sushiswap has deployed on multiple different blockchains other than Ethereum while also providing more features as limit order placing and lending. This has proven that so far there has been an addressable market for both protocols. Today, the total TVL of Sushiswap is around $5 billions while the one of Uniswap is around $8 billions[10].

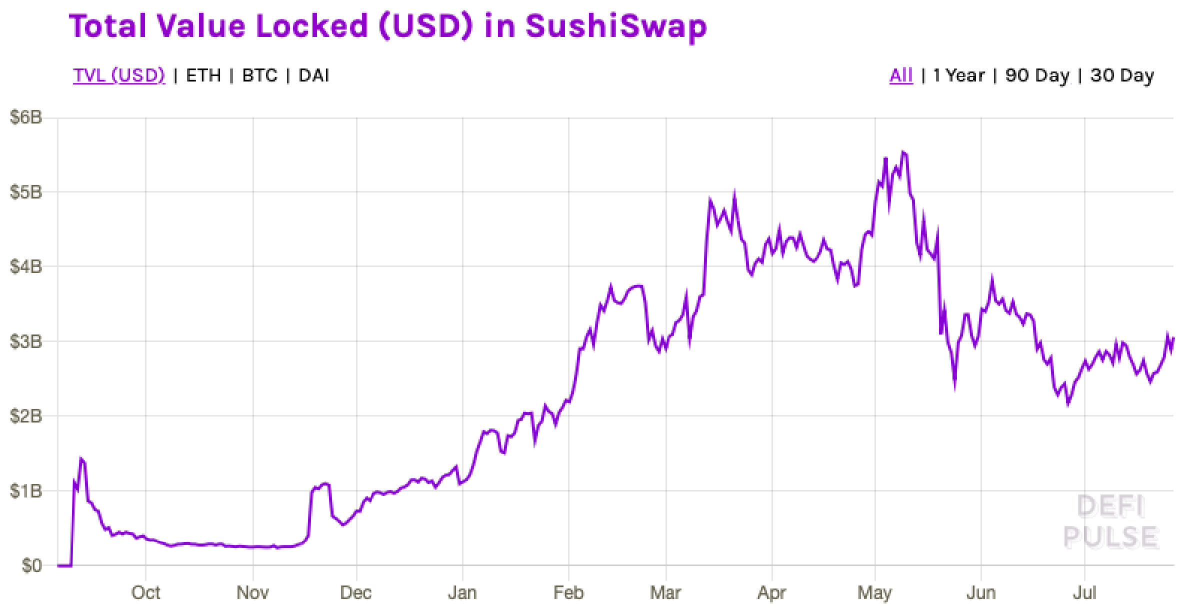

Figure 5.19: Sushiswap total value locked since inception (source: `https://www.defipulse.com`)

[10] https://defillama.com/protocols/dexes

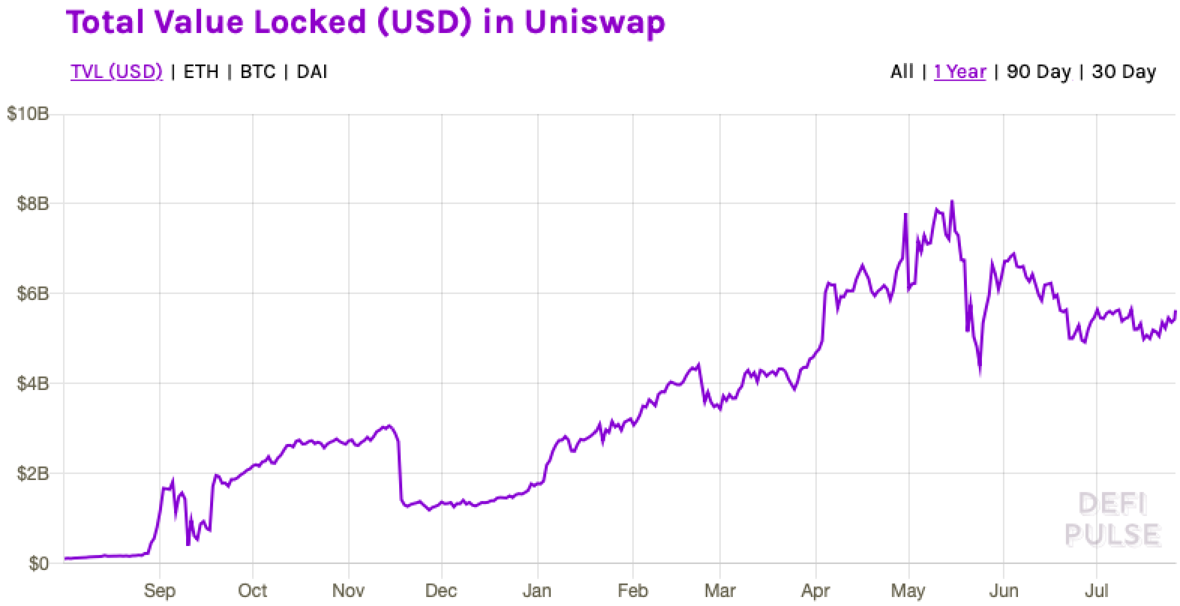

Figure 5.20: Uniswap total value lock for comparison with Sushiswap total value locked (source: https://www.defipulse.com)

Finally, Figure 5.21 below presents the weekly trading volume of Sushiswap which has only reached the $10 billion USD mark once, in may 2021. As visible, trading volume 'peaked' immediately in Sushiswap's first two weeks of existence given the novelty and attracting yeilds. However, after the initial period, trading volume decreased with users turning to Uniswap again until the end of 2020 from when both protocols have grown in volume (although Uniswap much more) quasi consistently. Nonetheless, having a weekly trading volume almost regularly above the $2 billion USD mark has proven Sushiswap's product market fit.

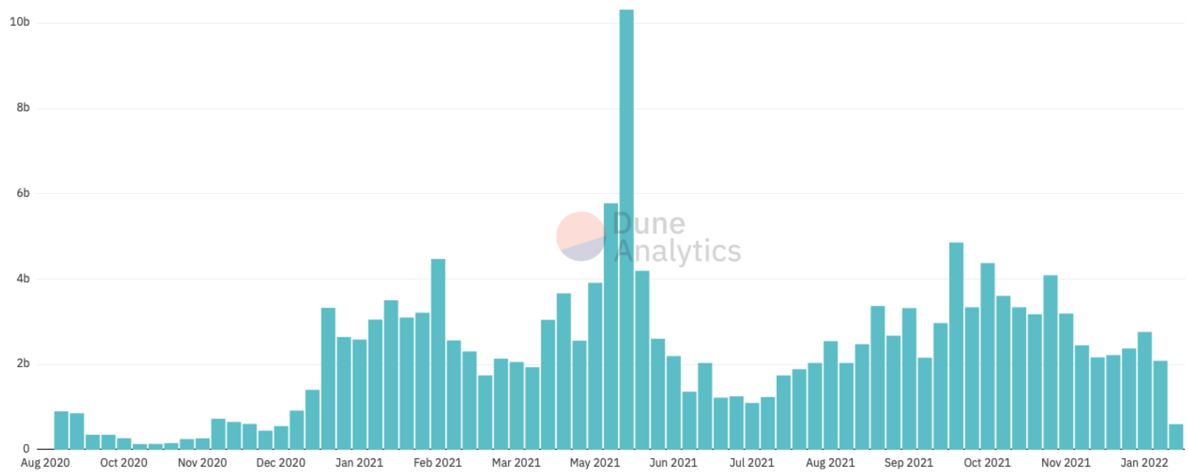

Figure 5.21: Weekly Sushiswap volume since inception in early September 2020

Community size

As for the size of the community, like most projects in the Defi space, Sushi has experienced an exponential user growth in the past year. In nearly 15 months, Sushiswap went from launch to more than 400 thousand users. This metric of course gives the total amount of users that have ever interacted with the smart contracts.

Whether that was for trading, providing liquidity or participating in governance, will be discussed in the next section. Even though, the growth of users has been quite linear and continuous over the past year, Sushiswap has only reached a fraction of Uniswap users which counts to date slightly more than 3 million users. This means that Sushi only counts 13% of Uniswap's total users. Which, with high probability, most are users of both protocols.

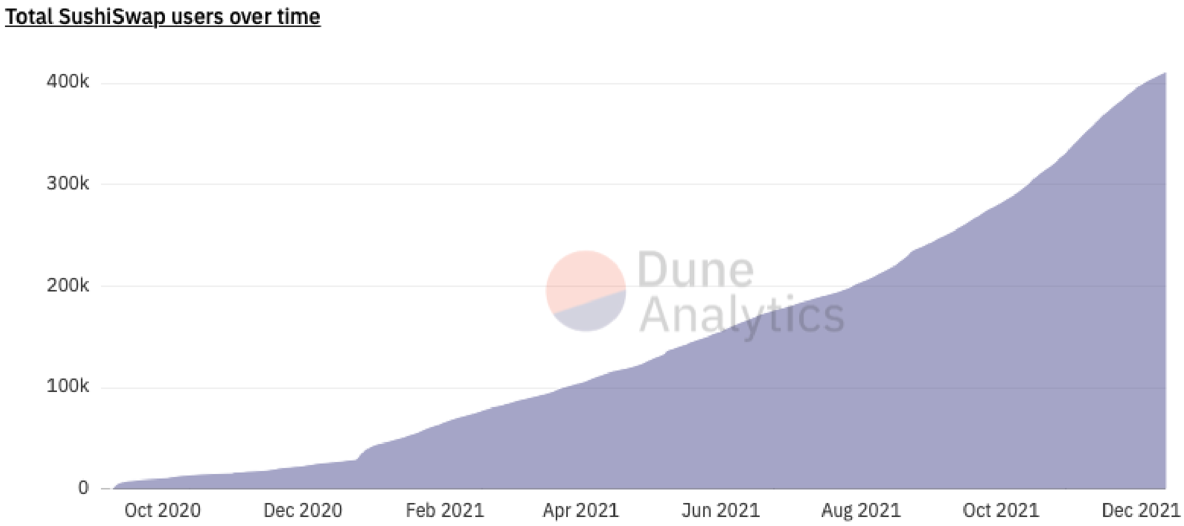

Figure 5.22: Cumulative amount of users of Sushi protocol since inception

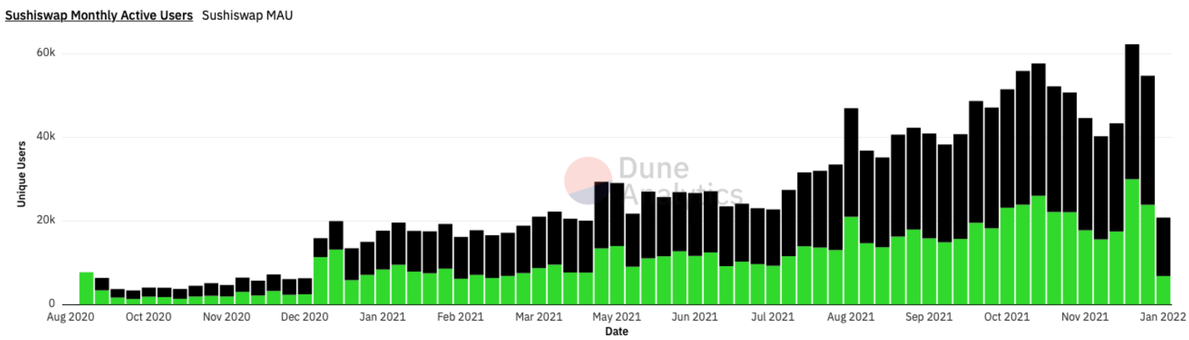

Figure 5.23: Weekly amount of old and new users utilizing the protocol

Community involvement

Given that the voting process is not conducted on chain, it is much more difficult to collect data for Sushi in order to evaluate the involvement of the community. Furthermore, for Uniswap one could also measure the involvement in governance by analyzing the amount of delegated tokens in the community. For Sushi, identifying the exact number of governance participants is more difficult given that one cannot track the amount of Sushipowah that has been obtained by either depositing liquidity in the Eth-Sushi pool or by depositing sushi in the sushibar in exchange for xsushi. One might argue that the amount of sushi staked in the sushibar is a measure of the amount of users participating in governance. However, one most also consider that there is a financial incentive for users to exchange sushi for xsushi, being the 0,05% of the total fees generated by the protocol. As a result, one is not guaranteed that each xsushi in circulation corresponds to a sushipowah token participating in governance. Nonetheless, it can work as an estimate given that no other data nor information is at hand.

To start, the amount of Sushi token to ever be emitted will be 250 million, one fourth of Uniswap's supply. Of this, 95% has already been emitted for a total amount of nearly 83 thousand Sushi holders. Of these, only 13 thousand actually own xsushi (whether for passive income, voting rights or both). As a result, only 15,6% of total Sushi holders also have access to governance. Furthermore, one can also notice from Figure 5.25 below that only 3 addresses hold more than 5 million tokens meaning that these addresses can singlehandedly propose and make proposals pass. Also in this case, there is a high degree of plutocracy.

Figure 5.24: From left to right: (i) amount of users holding sushi tokens, (ii) current amount of sushi tokens in circulation, (iii) total supply of sushi tokens

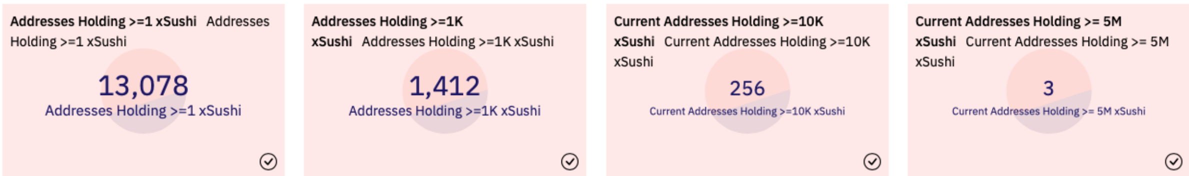

Figure 5.25: Amount of addresses holding sushi tokens from 1 to more than 5 million

Another way in which one could gauge governance participation is by analyzing the amount of xsushi tokens minted over time, as visible in Figure 5.26 below. As one can notice, the amount of xsushi has grown over the last year and just started to reduce in the past two months. Nonetheless, more than 60 million tokens were circulating around October of 2021. This translated in around 25% of the total Sushi supply.

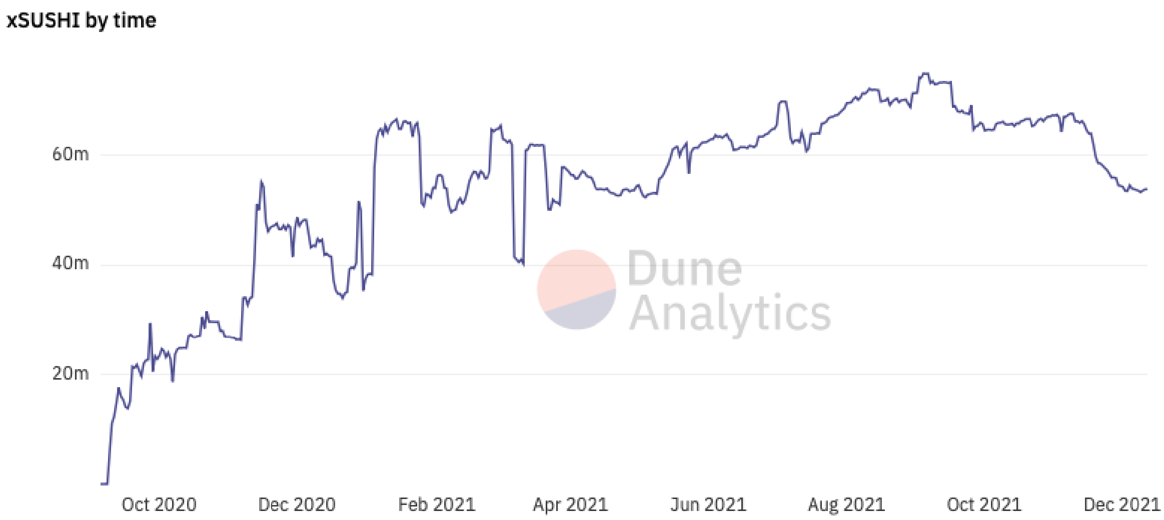

Figure 5.26: Total amount of xsushi tokens emitted over time

Token distribution

Given that Sushiswap was launched with a community oriented ethos, no sushi token had been previously allocated to early developers nor to early investors as venture capitals for the simple reason that there where none. As a result, the distribution of Sushi tokens has so far been solely as a reward for liquidity providers. Moreover, the team never released a roadmap for how sushi tokens were intended to be used and distributed over time. While this theoretically creates a levelled playing ground where any user can potentially have equal access to Sushi tokens, it has in reality proven that without a proper game theoretic design, wealth and power will naturally concentrate in the hands of a few individuals. This was also proven by data retrieved in Figure 5.25 that shows how only 3 wallets hold a disproportionate amount of voting power.

From the current distributions of both Sushi and xSushi tokens one can visualize that for sushi, 51% of the supply is held by only 4 wallets. While for xSushi, only 4 wallets hold 67.2% of the supply. This means that of the 58 million xSushi in circulation, almost 39 million are held by only four entities. As already demonstrated a number of times by the data, as in the case of Uniswap, Sushiswap experiences as high degree of plutocracy.

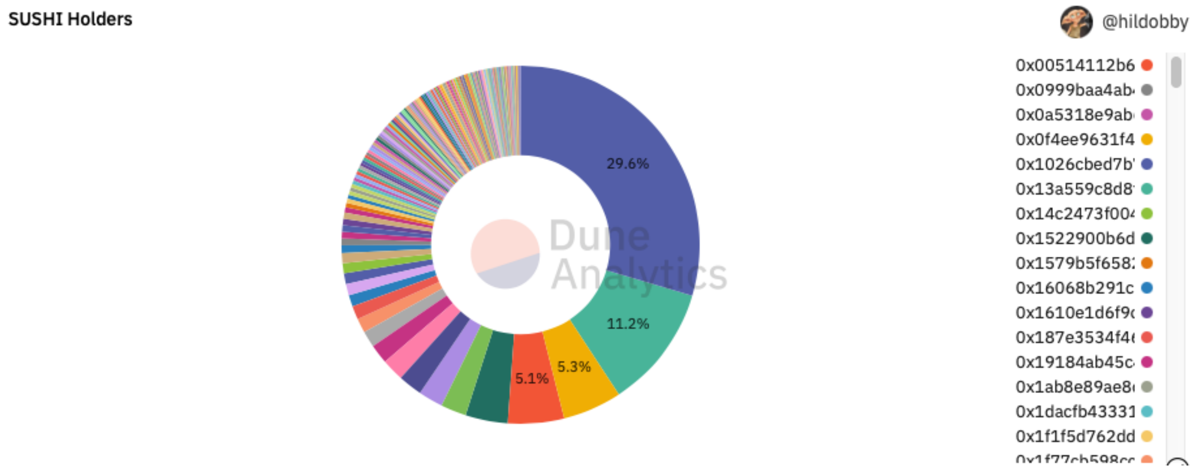

Figure 5.27: Current Sushi token distribution

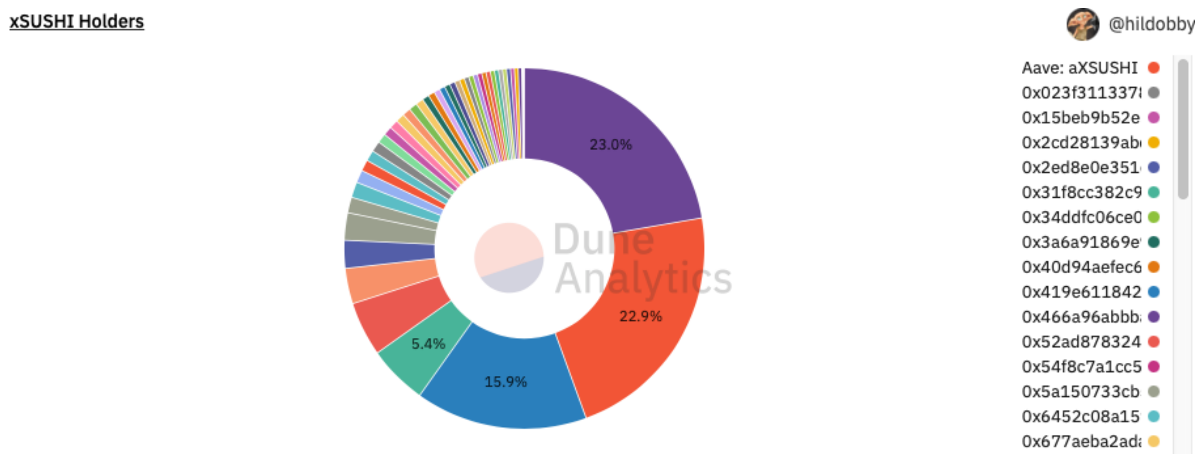

Figure 5.28: Current xSushi token distribution

5.6. Curve

Curve is an automated market maker (AMM) protocol first introduced in late 2019 that instead of offering the opportunity to create pools with any two (or more) pairs of assets, like Uniswap and Sushiswap, optimized for pools containing assets of equal value. In particular, Curve became the largest DEX for trading stablecoins. These are tokens that have their value pegged to national currencies hence, 'stable'. To date, the most utilized and known stablecoins are the ones pegged to the US dollar. The collateral behind these coins can be either actual dollars and treasury bills like in the case of stablecoins as USDT and USDC, or by other cryptocurrencies as in the case of DAI. As a matter of fact, Curve was initially named StableSwap by its founder (Egorov, 2019b). Given the lack of price volatility between the assets in the pool, the risk of impermanent loss for liquidity providers is significantly reduced. As a result, the protocol also charges less of the trading fees designated for liquidity providers in favor of traders.

By having minimal impermanent loss risk and charging lower fees than Uniswap and Sushiswap respectively, Curve is the ideal protocol for traders to exchange stablecoins and for liquidity providers to obtain a reasonable risk adjusted rate of return. This being said, Curve is to date the protocol with the highest total value locked among every protocol in the DeFi space. In fact, it is not only utilized by single users, but given its deep liquidity, also lending protocols as Aave have began to build on top of Curve's liquidity pools.

As will be also addressed in the following sections, Curve adopted some quite innovative solutions both for the actual exchange function of the protocol as well as for its governance. While the latter will be discussed in the 'rules in use' section, the former will be briefly outlined below. As introduced and explained in Chapter 4, automated market makers keep an equal value (when denominated in the same currency) on both sides of the pool by making the product of the quantity of coins remain constant. In other words following the function $x * y = k$, where x and y are the respective coin quantity and k is the constant. This function is also visible in Figure 5.29 below (red and blue dotted line). However, this particular function would be quite inefficient for trading assets of similar value given the considerable price slippage traders would experience when trading large amounts of capital. As a result, Egorov (2019b) developed a new invariant function that could reduce such slippage in AMMs. The blue line in Figure 5.29 below provides a visual representation of the function, also known as the 'stableswap invariant'.

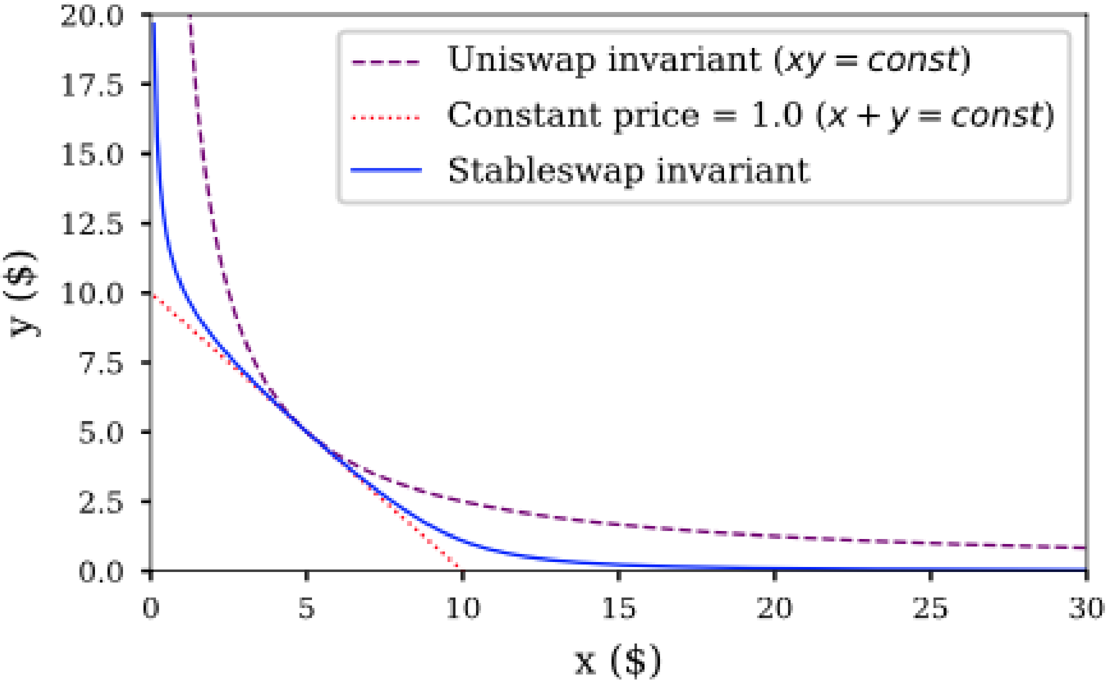

Figure 5.29: Comparison of constant function invariant with Curve stableswap invariant (Egorov, 2019b)

Rules in use

Position rules

Being a decentralized exchanges as Uniswap and Sushiswap, the same three sets of positions apply for users that interact also with the Curve protocol, namely: traders, liquidity providers and governance participants. These mentioned are the only set of positions that can be taken at a protocol level. Nevertheless, as in the case of Uniswap, Curve is also a privately held company, being registered in Switzerland. Its CEO is also its founder Micheal Egorov, and the company has received early stage funding from two different venture capital firms, which received a share of the total CRV governance tokens vested in 4 years. Proportionally, the share of tokens granted to early seed stage investors is much smaller than in the the case of Uniswap. There are also fewer shareholders and furthermore, the fact that these token are vested over a 4 year period prevents VC firms from accumulating disproportionate amounts of voting - hence, governance - power.

Boundary rules

The process of becoming a governance participant in Curve is fundamentally different from Uniswap, Sushiswap and the vast majority of all other decentralized finance protocols. Instead of having a one token one vote system (Uniswap) or a token staking mechanism (Sushiswap), Curve utilizes a time weighted voting system that grants voting power in proportion to the amount of time users commit to participate in governance. This system works as follows: the very first step to be done in the process of participating in governance is for users to own curve tokens, also known as CRV. These can be owned either by buying them on the open market or by receiving them as reward for providing liquidity in curve liquidity pools. Nonetheless, owning CRV is not enough. If a user does want to participate in governance he must then lock his tokens in a *VotingEscrow* smart contract that has a selectable locktime from a minimum of one week to a maximum of four years. As a result, the voting weight is equal to:

$$w = a * \frac{t}{t_{max}} \tag{5.1}$$

Where a is the amount of CRV tokens locked in the escrow, tmax is the maximum lockable time which is four years, and t is the current time left for locking expiration (Egorov, 2019a). From the formula above one can therefore notice that voting weight in curve is both amount and time dependant. In particular, the voting weight will reduce linearly with time until expiry, as visible in Figure 5.30. This system was created in order to prevent users from buying large amount of tokens at any given point in time and having large voting power as a result. In addition, for users to have a significant voting power they must lock their tokens for a considerable amount of time therefore committing with their time to holding CRV tokens and participating in governance. This system is fundamentally different from the ones of the projects described above and as it provides a more trustworthy and secure form of governance.

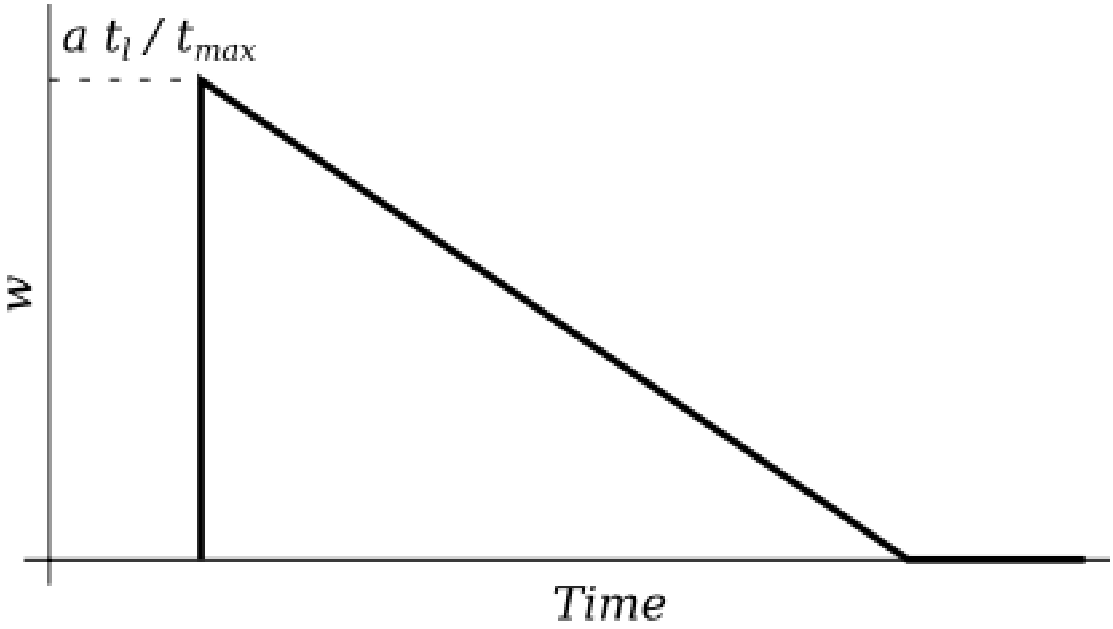

Figure 5.30: Curve voting weight linear decay over time (Egorov, 2019a)

Choice rules

Given the difference in a number of fundamental governance aspects, the type of choices participants can make are also different to some extent. The very first difference with protocols like Uniswap is that instead of choosing whether to delegate or not, users in curve choose the amount of time they want to lock their tokens, as a result choosing their voting weight. In curve users cannot choose to delegate their voting power to other participants, or at least not directly. What users can do is to send their CRV tokens to other entities and let the latter lock their tokens and receive governance rights. This will be further discussed in the payoff rules section. Moreover, there is also a difference in the type of proposals users can vote on. In the governance of Curve, users can only vote on collective choice rules, or in other words, on rules that affect how the protocol works on an operational level. For instance, participants can only vote on reward implementation for pools or changes in parameters of the protocol. As a result, this means that constitutional level rules were set and are decided upon exclusively by the founder and core team.

Aggregation rules

In the voting system of Curve there are two different aggregation rules for two different voting categories, namely: ownership and parameter changes. The former concerns mostly the implementation of new gauges (pools that can receive CVR rewards), while the latter concerns changes to protocol parameters as the increase or decrease of fees. These two voting categories have different thresholds for proposal passing and quorum. Ownership votes need at least 51% of favourable votes and a quorum of 30% of the total tokens that can vote. On the other hand, parameter votes need 60% of favourable votes in order to pass and a quorum of 15%. Finally, in order to make a proposal, a given wallet address needs to hold at least 2500 veCRV tokens.

Information rules

Information channels are quite similar to the ones of the projects earlier described but information flow and proposal submission is not as structured as in the case of Uniswap. Nevertheless, Curve also utilized the same three information channels. First, Discord application is the one most utilized by the community and is the go to venue for users to ask any sort of question as well as to create community culture. Second, the Curve community forum is the venue utilized to discuss actual protocol and governance proposals. Third, Snapshot - as in the case of Sushiswap and Uniswap - is the off chain mechanisms utilized for preliminary voting in order to practically gauge (temperature check) the agreement of the community on given changes. Finally, once proposal reach sufficient consensus they are voted on, on the official on chain curve voting mechanisms also presented in the Figure 5.31.

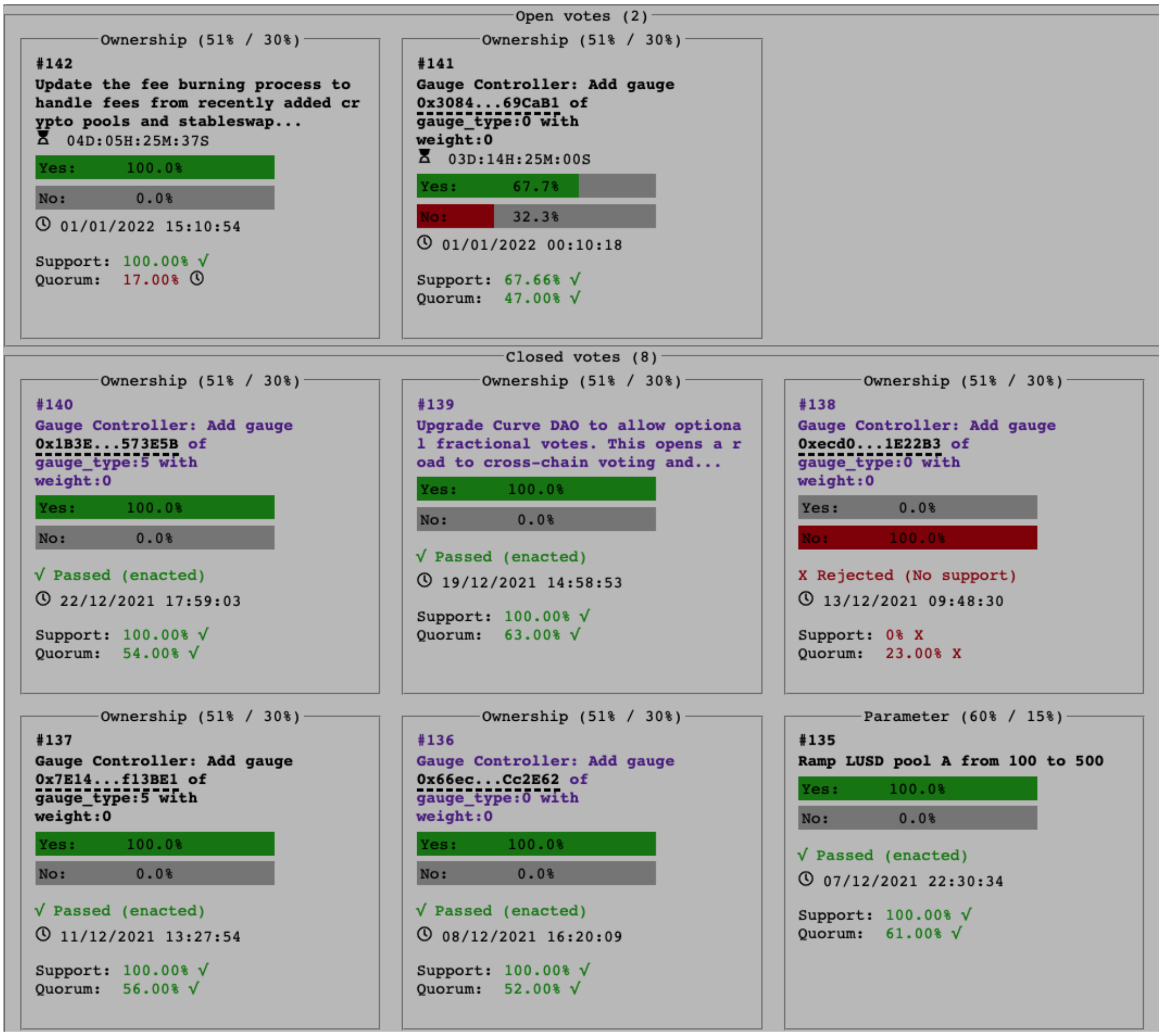

Figure 5.31: Proposals and official voting portal of Curve (source: `https://dao.curve.fi/dao`)

Payoff rules

One of the features of the Curve protocol that differentiates it the most from other decentralized exchanges (and applications in general) is its innovative incentive scheme. On top of the fees received by liquidity providers - payed by traders - the protocol also rewards various pools with CRV tokens on a constant basis, therefore increasing the incentive for users to deposit their liquidity in such pools. However, the protocol does not reward each pool equally. Users themselves can 'vote' with their veCRV tokens which pool they prefer to receive more rewards. This mechanism has initiated the so called 'Curve wars' which develop as follows. In order to incentivize users in governance participation, the protocol developed a way to incentivize CRV locking. On top of voting rights deriving from veCRV users can utilize those same veCRV to boost CRV rewards in pools of their preference. For instance, if a user has provided a significant amount of liquidity into the tricrypto pool (one of Curve's largest pools containing USDT-USDC-DAI), that same user is incentivized to buy CRV tokens, lock them in the voting escrow and utilize the veCRV tokens to vote and boost the CRV rewards in the tricrypto pool. Reward allocation is voted upon once a week and a pie chart of the reward weights per pool is provided below in Figure 5.32. This system has created an increasing demand for CRV tokens, and at the time of writing near half of them are locked in the voting escrow as will be discussed in the next sections.

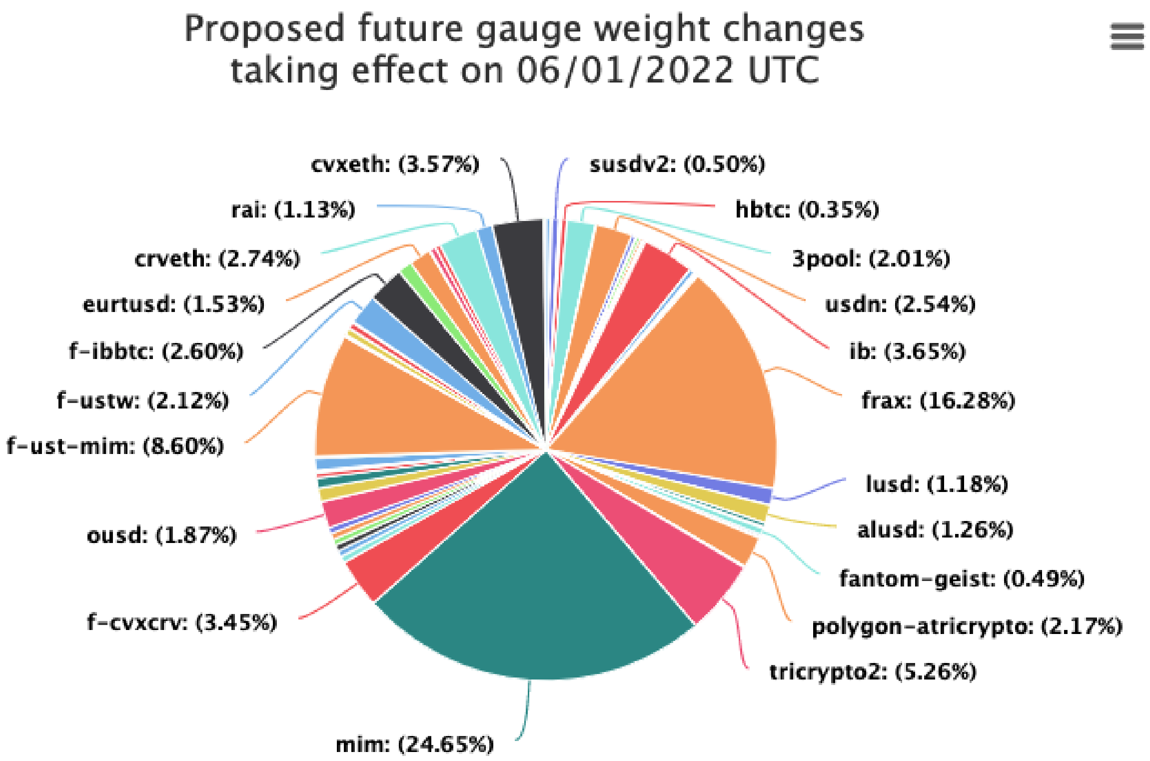

Figure 5.32: Curve gauges voting distribution (source: `https://dao.curve.fi/gaugeweight`)

Scope rules

Both the incentive scheme described above as well as the token lock mechanism utilized to grant voting rights can be seen as scope rules given that their 'scope' is, in the first case to incentivize liquidity providers in participating in governance, and in the second to secure the voting system from malicious actors. Also, the time weighted voting system was developed with the scope of incentivizing commitment of governance participants. Finally, the utilization of Snapshot as temperature check mechanisms has as scope the gauging of potential proposal implementations.

Evaluative criteria

Total value locked & volume

As visible from Figure 5.33 below, the total value locked in smart contracts of Curve started to pick up around mid 2020, at the beginning of 'DeFi Summer'. Since then, the TVL reached a value of $2.5 billion USD at the end of 2020, which then eight-folded in 2021 reaching a total of $20 billion USD. Moreover, Curve has been deploying its stableswap liquidity pools on other blockchains as well as Avalanche, Polygon and Fantom among others. To date, on top of the $21 billion USD locked on the Ethereum blockchain, Curve counts for an additional $3.38 billions locked on seven other chains. This makes of Curve the protocol with the highest total value locked among all DeFi protocols, locking nearly three times the value of the second biggest protocol by TVL (Uniswap), and accounting for nearly 10% of the total value locked in all DeFi protocols[11].

[11] https://defillama.com

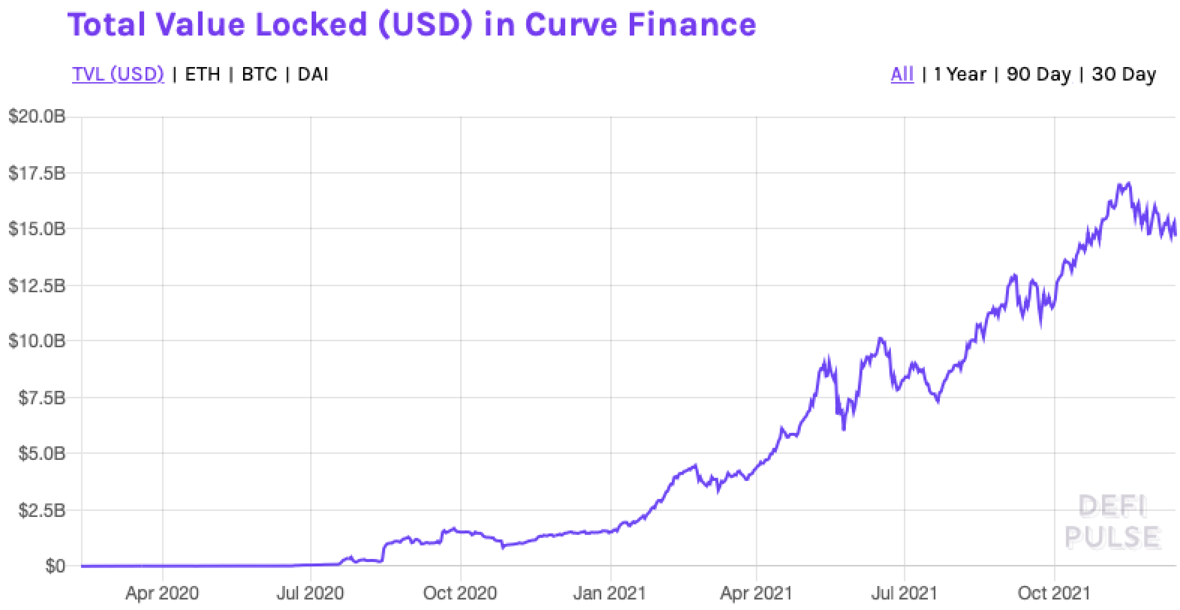

Figure 5.33: Curve total value locked since inception (source: `https://www.defipulse.com`)

Given that the very vast majority of trades on Curve are between stablecoins holding their value pegged to the dollar, the volume on Curve is calculated to be considerably lower than on exchanges that trade any pair of tokens like Uniswap and Sushiswap. Since the start of its 'wide' adoption utilization in mid 2020, Curve has had an average weekly volume of around $1.5 billion dollars. Nonetheless, the protocol experienced two major weeks during its existence where its traded volume surpassed the $3 billion dollar mark. The first one in mid October 2020 and second one in mid May 2021 respectively. Overall, the increasing volume over time has proven product market fit for a stableswap protocol like Curve.

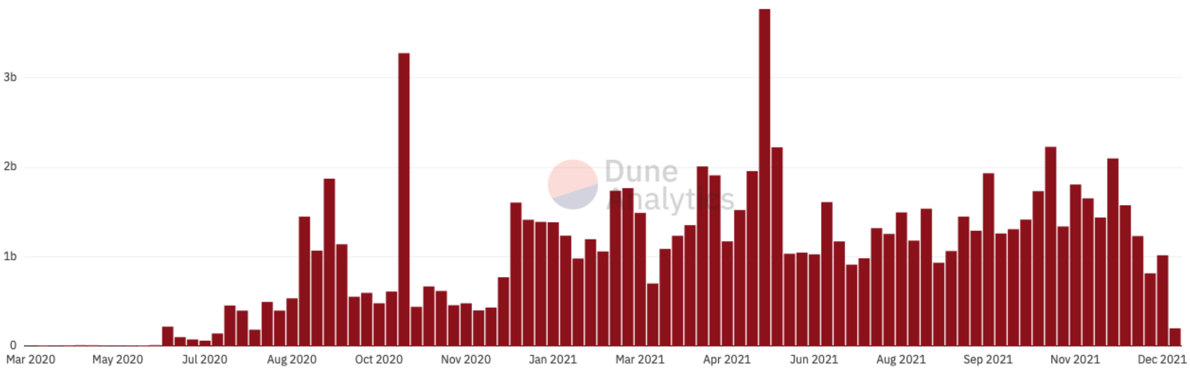

Figure 5.34: Weekly Curve volume since March 2020

Community size

The size of the community, or the amount of users that have used the protocol over the past year and a half are around 53 thousand. Figure 5.35 shows how the cumulative amount of users has grown (quasi) linearly since DeFi summer to date. On the other hand, Figure 5.36 shows the amount of weekly old (black) and new (users) that interact with Curve either to swap or to provide liquidity. As noticeable, the protocol experienced sudden surge in utilization during DeFi summer - perhaps due the introduction of incentive schemes - while after July 2021 to amount of new and old users has almost linearly been declining, probably in favour of other protocols on other chains.

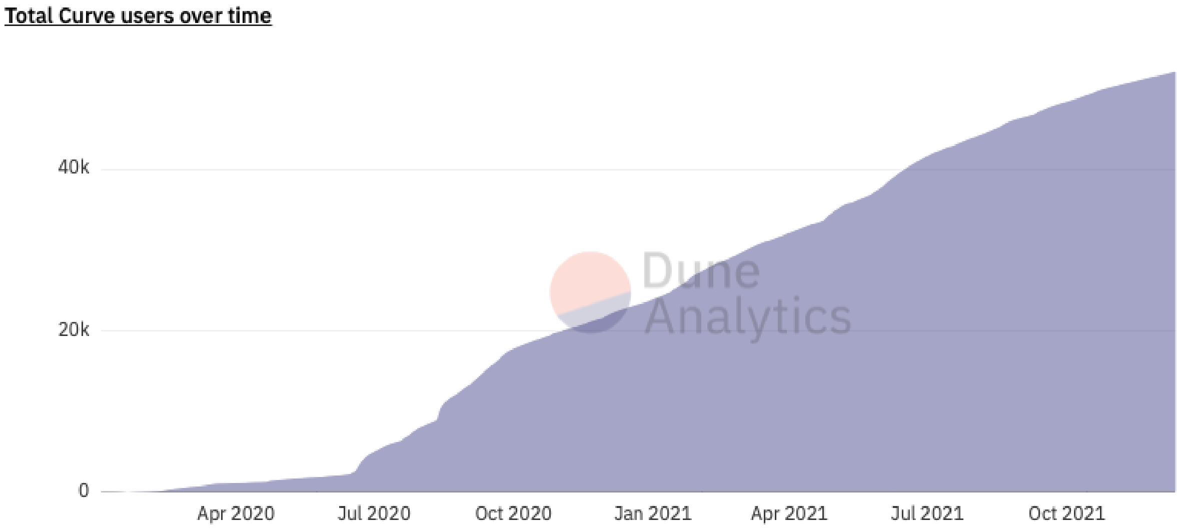

Figure 5.35: Cumulative Curve user base growth

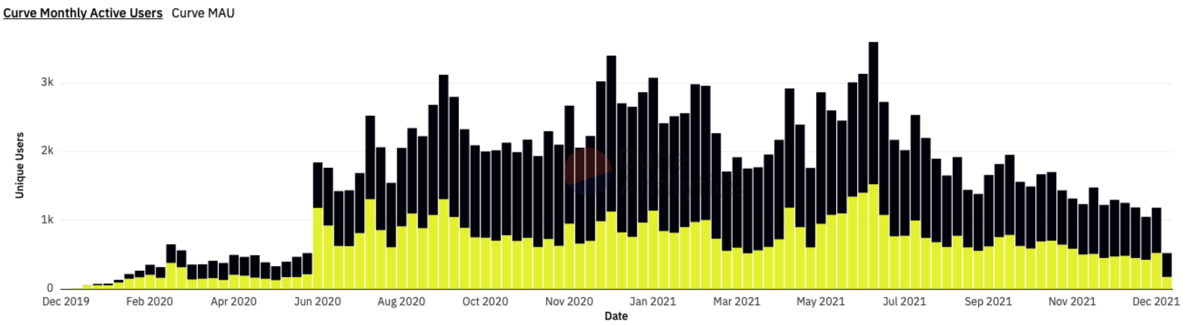

Figure 5.36: Weekly amount of old and new users utilizing Curve protocol

Community involvement

As for the vast majority of the space, the different metrics that can be utilized to gauge community involvement change from project to project. In the case of Curve, one can obviously utilize the amount of escrowed CRV tokens as a proxy to measure involvement. Nonetheless, given that veCRV tokens are also utilized for reward boosting, one might argue that a number of users utilize the latter only as financial incentive and not for governance participation as much. As a result, one can also measure voting participation in the different polls to calculate the % of escrowed tokens in governance and have a more accurate measure of community involvement.

Retrieved directly from the voting portal of Curve Dao, Figure 5.37 shows how of the entire Curve tokens in circulation, slightly more than half have been locked in the voting escrow, for an average amount of time of 3.64 years, which means that most of the users that have locked their tokens have chosen to commit for nearly the maximum amount of time possible.

```
Total 🌈 CRV vote-locked: 404,211,183.80
Percentage of total CRV Locked excluding voting escrow: 103.13%
Percentage of total CRV Locked: 50.77%

Total veCRV: 367,772,105.86
Average lock time: 3.64 years
```

Figure 5.37: Percentage of total CRV tokens locked, total amount of veCRV minted and average locking time (source: `https://dao.curve.fi/locker`)

Figure 5.38 provides a visual representation of the numbers displayed in Figure 5.37 where the blue line represents the amount of locked CRV tokens over time, while the red line tracks veCRV emissions. Given that 1 CRV token equals one veCRV token only when the former is locked for 4 years, the fact that these two lines have grown quasi in parallel suggests that most of the tokens have been locked for the longest period of time. However, one must recall that veCRV tokens are also utilized to vote on the pools that must receive the most rewards. On this regards, Figure 5.39 below provides a visual representation of the weekly voting distribution. Each column of the table represents the voting results of the week. Each colour represents a different pool. As visible, over time some pools have lost voting preference and therefore rewards. This could be explained either by participants changing their vote, or by new participants concentrating high amount of voting power and therefore changing significantly weight results.

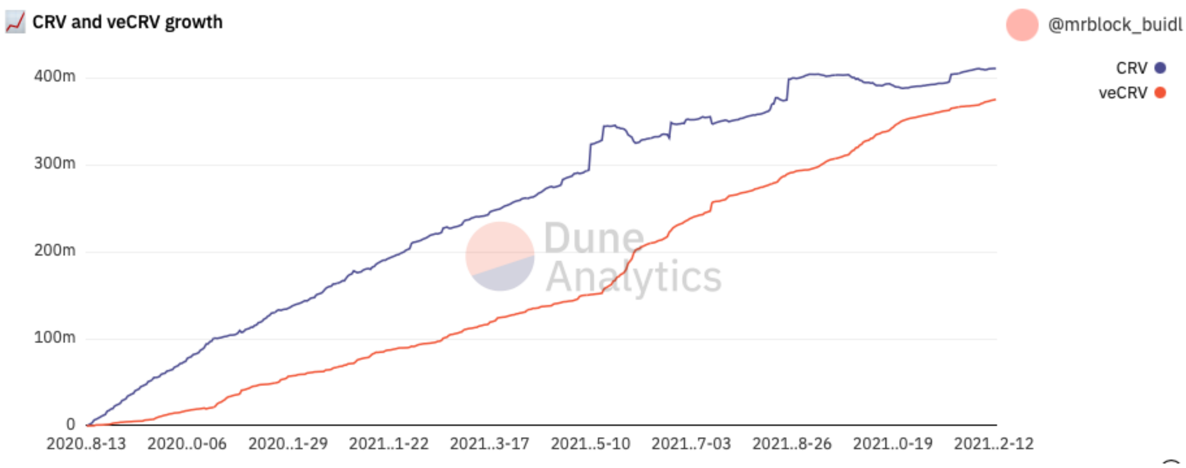

Figure 5.38: Comparative growth of Curve tokens and voted escrowed tokens

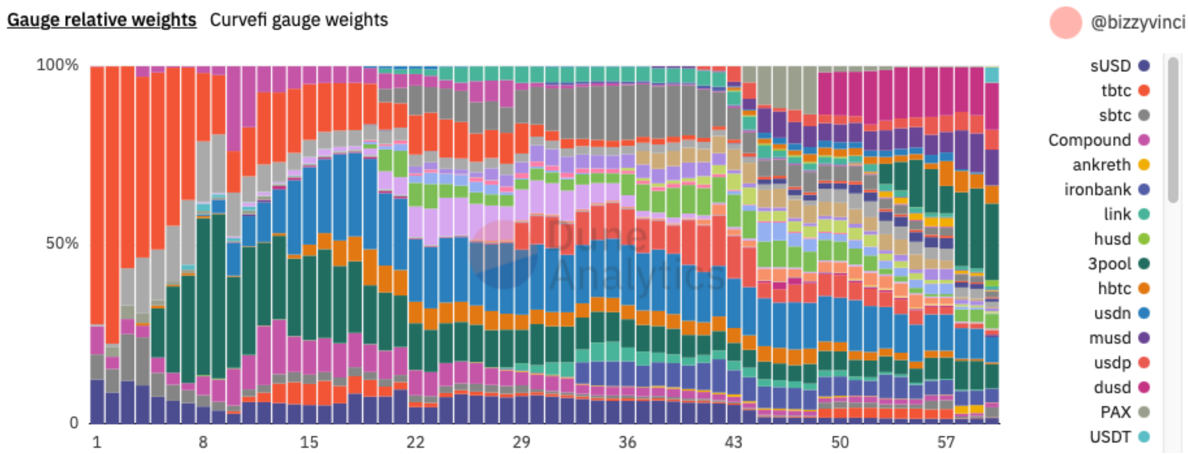

Figure 5.39: Curve gauges voting distribution over time

Given the economic incentive for locking CRV tokens described above, one must therefore analyze voting participation in different polls in order to actually have a measure of governance participation. So far, there have been 145 voting proposals to vote on. For the purpose of this analysis, only the proposals of the past three months will be analyzed as results already show to be statistically significant. From early October there have been 30 proposals out of which 25 have passed and 5 not. However, the average number of voting addresses has been 11, where 41 has been the maximum number of addresses voting in a single proposal while 1 has been the lowest. Given that out of these 30 proposals, quorum has averaged at 52%, one would assume that only half of the participants are active in governance. Nonetheless, since only 11 addresses hold more than half of the voting power, governance involvement is significantly less than that.

Token distribution

As inferable from what discussed in the previous section, the token distribution of CRV is all but decentralized. In fact, it presents incredibly high degrees of centralization. The initial token distribution was designed to be as presented in Figure 5.40 below. Where, 62% of the total tokens where to be distributed to the community through liquidity mining incentives. 30% of the tokens to the shareholders that invested early in the company, and the remaining 8% to be distributed between employees and community reserves. Furthermore, the tokens allocated to shareholders and core team are vested linearly vested in four years as presented in Figure 5.41 below.

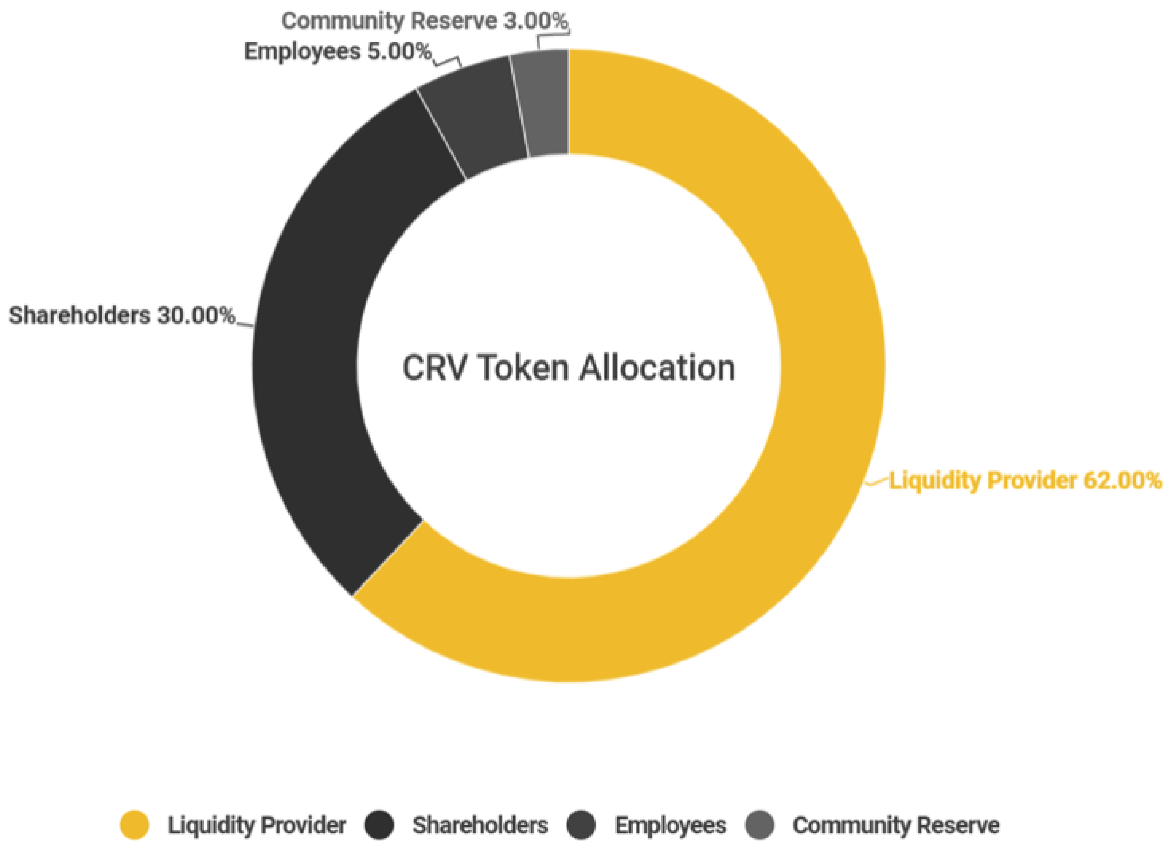

Figure 5.40: Curve initial token distribution (source: `https://resources.curve.fi`)

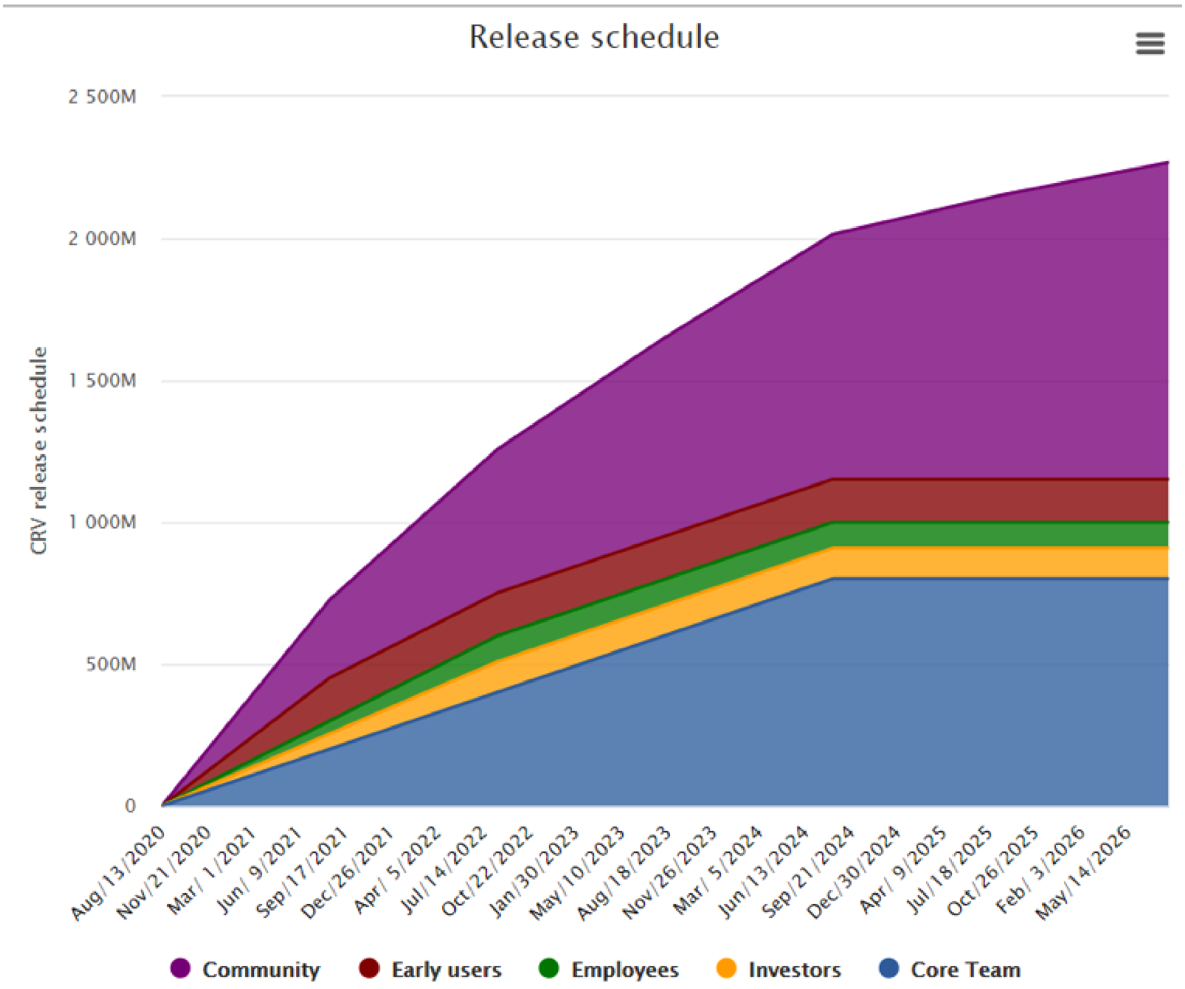

Figure 5.41: Curve token release schedule (source: `https://resources.curve.fi`)

Nevertheless, economic incentives deriving from veCRV tokens has propelled its demand more than the granting of governance rights instead. Given that veCRV holders can vote on which pools must receive most rewards, a number of other projects have been accumulating as much CRV tokens in circulation with the goal of receiving rewards in pools of interest. Of these project, Convex has been thus far the one that has managed to accrue most tokens, holding to date nearly 180 million veCRV tokens, or nearly 43% of its supply, as better visible in both Figure 5.42 and Figure 5.43 below. As a result, Curve governance is far from decentralized and also holds a high level of plutocracy.

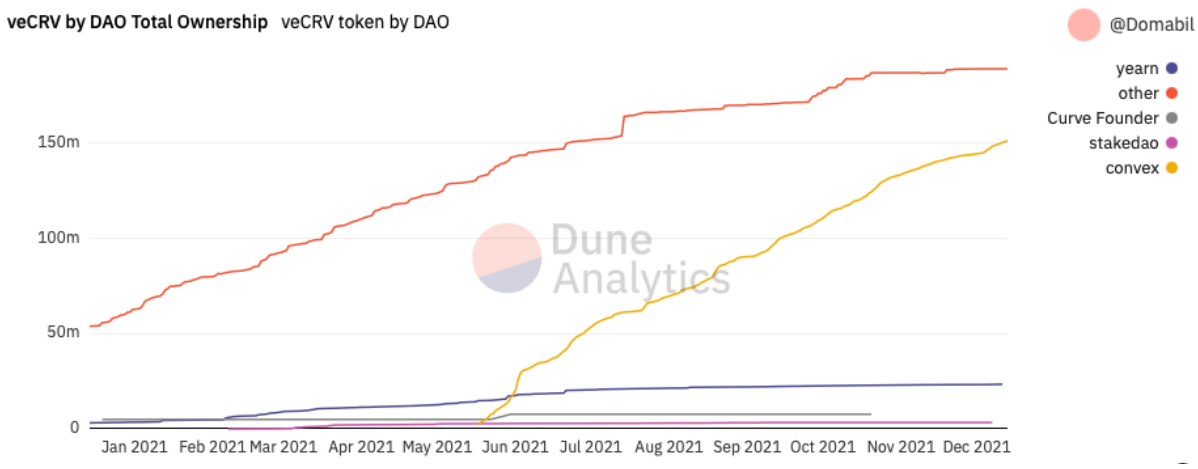

Figure 5.42: veCrv token distribution over time

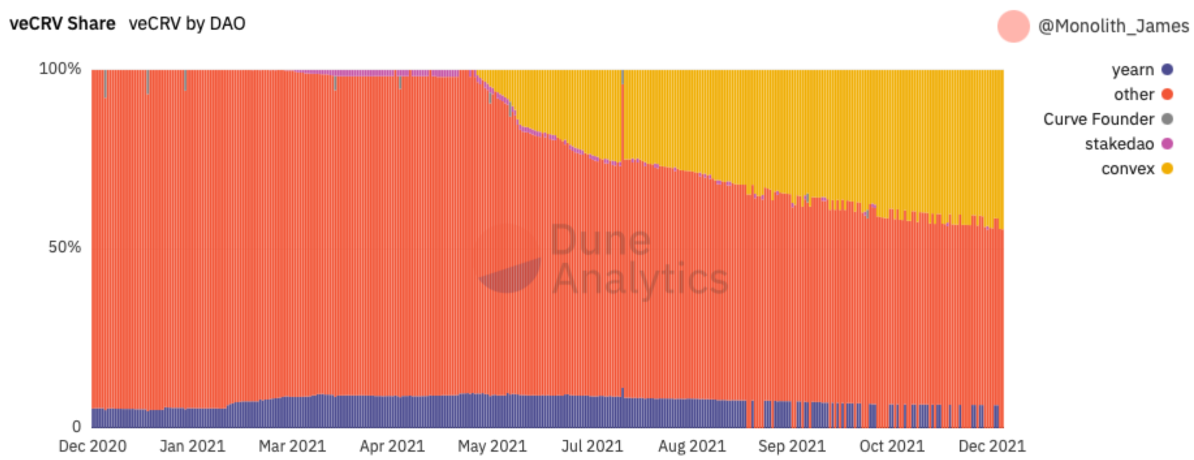

Figure 5.43: veCrv token distribution over time in percentage between Convex, Stakedao, Yearn and others

5.7. Results and Discussion

The purpose of the following section is to present the results obtained from the analysis conducted above and to answer the main research question: *'What institutional innovations does blockchain technology introduce to the exchange of financial assets?'*.

Undoubtedly, the rules in use pertaining the 'external variables' of the IAD framework are the building block that, more than any other component of the framework, provides useful insights into the internal coordination structure of the different communities. Furthermore, it allows analysts to differentiate between the protocols the best. Starting with the horizontal analysis of the rules in use, the ones spanning from position to scope rules, the categories that turned to be more telling about the governance of the projects and performance of the protocols were: boundary and payoff rules.

As exposed in previous sections, each of the projects analyzed is characterized by different boundary rules: different actions participants must take in order to become a governance participant. In the case of Uniswap, users are simply required to delegate their governance tokens (UNI). Delegating tokens is not incentivized by any means nor does it require any commitment in time. For Sushiswap, users must stake their tokens in a yield producing escrow in order to obtain governance (voting) power. Like Uniswap, this action does not require any established time commitment, however it is incentivized. Finally in the case of Curve, users must both stake their governance tokens in a yield producing escrow and at the same time indicate for how long are they willing to stake their tokens. The longer the time period selected, the higher the voting power. As a result, in order to participate in governance, users are both economically incentivized and required to commit in time.

The results from these three different mechanisms is that: of the total tokens in circulation each project has, 32%, 25% and 51% for Uniswap, Sushiswap and Curve, are respectively utilized for governance participation. What these results suggest is that, in the best case, only half of the tokens meant to confer voting rights are actually used to do so. Furthermore, Curve has actually one of the most well developed incentive mechanisms as outlined in its dedicated section, as a result the majority of the tokens are locked for economic incentives rather than governance participation. This proves that so far, governance tokens have been mostly seen and utilized as tradeable assets rather than tools for governance.

Payoff rules are the second set of rules that differ the most between protocols. In fact, the three of them have implemented diverse game theoretic models and incentive schemes to both stimulate governance participation and liquidity attraction. In order, Uniswap does not directly incentivize by any means governance participation. In other words, there are no established financial rewards for participants to propose or vote in governance or protocol updates. Not directly, at least. As a matter of fact, a governance proposal was introduced to increase the trading fee from 0.3% to 1% for certain pools having low liquidity and volume. Recalling that trading fees are payed out to liquidity providers of the pool, a wide number of governance participants who were also liquidity providers voted in favour of this proposal as is would allow them to gain more profits by depositing capital in such pool. Therefore, these participants had an economic incentive. Furthermore, even if Uniswap does not incentivize voting, the amount of delegated UNI has increased over time reaching today nearly a third of the total tokens in circulation.

The case of Sushiswap clearly shows how the right set of payoff rules can potentially disrupt entire projects. In fact, by offering the very same type of product but with higher yields for liquidity providers, Sushiswap had managed to steal liquidity from Uniswap twice in its first two months of existence. This is clearly visible by comparing total value locked in Figure 5.6 with Figure 5.20 and the increased trading volume on Sushiswap on those dates, as in Figure 5.21. Also noticeable how, regardless of initial 'vampire attacks', both protocols have grown in both TVL and trading volume ever since. Interestingly enough, even if locking tokens for governance is incentivized in the Sushiswap protocol, in proportion, more tokens are locked for governance in Uniswap - where there are no incentives - rather than Sushiswap. This could mean that participants in Uniswap have higher conviction in the project, even if less financially rewarding, and therefore have more interest in the governance of it. The higher TVL and volume of Uniswap over Sushiswap may also seam to suggest so.

Finally, as aforementioned the payoff rules implemented by Curve have turned to be so successful that not only does the protocols enjoy the highest TVL in DeFi to date, but many of the new projects coming out in the space are copying its incentive scheme model. In simple terms, the more tokens users lock and the longer they lock them for, the higher the claimable economic reward. These incentives have also translated in more than half of the tokens being committed for governance. Nonetheless, as presented in the 'community involvement' section for Curve, only eleven addresses on average vote for proposals and hold as well half of the total voting power meaning on one hand that voting participation is extremely low, and on the other that voting power is significantly concentrated, as will be further explained below.

Other than the specific rules in use outlined above, some of the 'attributes of the community' can also provide a number of insights on the governance of these protocols. As introduced in previous sections, Uniswap and Curve received funding from early stage venture capital investors in exchange for equity and governance tokens, while Sushiswap was born since inception with a community centered vision and therefore had no governance power pre-distributed to any large early investor. In institutional terms, this means that at launch there was one actor less in the action arena. Eventually, a number of venture capitals did invest large amount of capital in Sushiswap - hence obtaining substantial voting rights - however, this only occurred at a later stage. The presence or not of venture capitals has turned not to have equal impact on each community as will be discussed below.

By now taking the vertical approach in rule analysis one can notice that of the three projects analyzed Curve is the only one that allows the community to vote only on a collective choice level, meaning the community can decide and vote on changes to the operations of the protocols but not on how the consensus and voting process should work itself. On the other hand, both Uniswap and Sushiswap allow the community to participate in constitutional level decision making where participants can propose changes to the decision making process. For instance, in Uniswap the community successfully voted for a reduction in the quorum necessary for proposals to pass. While the entire Sushiswap community has even voted more than once on which individuals must or must not form part of the core developer team. Intuitively, one might guess that projects having venture capitals included in the community would be the ones that would not allow constitutional level rule making, as it is in the interest of venture capitals to protect their investment by keeping decision making power in the hands of few trusted members. While this has turned to be true for Curve it is not the case for Uniswap. However, thus far the most innovative governance mechanism has been adopted by Sushiswap - being developed with decentralization ethos at heart - where the community at large gets to decide on every aspect of the protocol and along the three levels of analysis in the vertical approach.

Useful insights can also be drawn by analyzing the distribution of governance tokens within the different communities. Even though the entire ethos of the space is to build applications that avoid power centralization, from the analysis conducted in the previous chapters it results quite obvious that, at least for the projects analyzed, there is a considerable high degree of power centralization through concentration of tokens. For Uniswap, even though the initial token distribution was designed to be 60% to the community and the rest between early investors and core team, as of today only ten entities hold cumulatively 46% of the supply. While the first 50 entities, hold cumulatively 98% of the total voting supply. This means that from a total of 8721 addresses that can cast at least one vote, 0,05% of them hold almost all the voting power. The case for Sushiswap does not hold any better where only 4 addresses actually control nearly 70% of the voting power, therefore singlehandedly being able to propose and vote and make pass any sort of proposal. The case of Sushiswap does however highlight an interesting factor, being born as a community oriented platform, Sushiswap did not have an initial token distribution where early VC investors were granted a large part of the supply as in the case of Uniswap. Nonetheless, after nearly a year and a half from launch the token distribution is arguably even more centralized than the other projects. This meaning that power centralization is not only a function of initial distribution. Finally, Curve also hold a significant power centralization issue as one single player, Convex, holds basically almost half of the entire veCRV supply. In the case of CRV, token accumulation mechanisms compound given the particular economic incentive behind it as well. The more users accumulate veCRV tokens, the more they are incentivized to accumulate them. As in the case of Uniswap, Curve had an initial token distribution where 62% of the distribution was intended for the community and the rest being vested for shareholders and core team. As a result, one can infer that each protocol is characterized by high power concentration and therefore governance is far from being decentralized as of today.

The results from the token distribution model presented above suggests that while new projects launching on blockchains aim at having both a decentralized architecture and governance, in reality only the former is true (if on Ethereum). In particular, even in cases where a large amount of users hold at least small fractions of voting power, participation in governance by voting has resulted extremely low for the three project analyzed. In numbers, in the case of Uniswap in the last half of the proposals, on average only 92 delegates have voted. Meaning only 1% of the addresses that can vote, do so. Furthermore, in Curve voting participation is even worse given that on average in the last 40 proposals only 11 addresses have voted. Well under 1% of the entire veCRV holders. Protocols are therefore characterized by low governance participation.

There are at least three potential reasons that can explain such voter apathy. The first one is of course the large power centralization outlined above. Having players with large voting power is a deterrent for smaller players to vote as they know their vote would have a negligible impact. The second reason is the strong misalignment between governance and economic incentives. Most participants lock their tokens in governance conferring positions only because of the rewards they can claim rather than actual governance participation. Third and final, voting and participating in governance requires a degree of knowledge that at this point in time most of the participants lack. Users mostly access this space as investors in search of high yields, understating the technical and governance innovations requires time and understanding many do not dispose.

The results from the analysis above seem to suggest that, instead of developing new forms of governance, current decentralized exchanges are actually resembling hierarchical forms of governance as corporate governance, where a restricted amount of members, usually the core team and a number of early investors, take all of the strategic decisions and decide where to steer the community and protocol. In this regard, following the theories of Coase (1937), the remaining paragraphs of this section will answer the fourth sub research question *'In virtue of Coase's theory, has the reduction in transaction costs associated with financial product exchanges actually modified their governance structure?'*.

Shleifer and Vishny (1997) define corporate governance as the form of governance that 'deals with the ways in which suppliers of finance to corporations assure themselves of getting a return on their investment'. This definition can apply for both Uniswap and Curve that have received investments in early stages from venture capital firms. The power centralization these communities experience could be regarded as a mean by which the core team assures early investors a return on their profit. While this could hold true for these two protocols, on the other hand in the case of Sushiswap where early investor received any allocation, power centralized anyway. As a result, one could argue that power centralization is more a function of human nature rather than early token distribution. Another angle for defining corporate governance derives from Jensen (1986) definition of agency problem. Which considers the separation of ownership and control of a firm between managers and shareholders. While agency problem holds very true and is existing in many traditional companies, it still hasn't manifested as a problem in the governance of the projects analyzed as in their managers - usually the core team of developers - are at the same time large shareholders and are deeply vested and invested in the project itself. As a result, their incentives are aligned with the shareholders therefore neutralizing agency problems.

In sum, while its true that as of today most protocols in the space are resembling different forms of corporate governance, it is also true that these same projects present elements of innovation that could foster different institutional regimes in the future. One example is the fact that any user that buys or earns a governance token is entitled to vote, propose or accrue voting power by vote delegation. Or that any user can have voting power delegated and therefore accrue relevance in governance. Furthermore, one must recall that in these virtual communities, more often than not users interact behind anonymous names. As a result, users that receive vote delegations because of their contribution and ideas shared in the community, are being rewarded by actual merit, rather than reputation or prejudice. Another example is the fact that new projects are already testing new forms of voting, as in the case of Curve, where voting power is not only a function of the amount of tokens a given user holds but also on the amount of time he commits in the community. Given the relatively low costs of institutional entrepreneurship allowed by blockchains it is very likely that new forms of gauging preferences will be experimented in the future. By assessing that the communities of the protocols analyzed have only grown in number since inception, no matter performance, governance or yield suggests that institutional innovation among others have merely started. In conclusion, the writer argues that the likelihood of discovering and implementing new institutional regimes utilizing blockchain technology is extremely high, and the reason why it may not be apparent to some yet, is that these projects today are still at the very first stage of iterative institutional development.

Reflection

The purpose of the following section is to reflect on the Institutional Analysis and Development framework developed by (Ostrom, 2010) as method for analysing the governance of decentralized exchange applications. The methodology was chosen given its flexibility and impartiality in analyzing governance mechanisms. This makes of the following research the first of its kind, since until this point the governance of blockchain applications has been studied purely by comparison with existing institutional structures (Allen et al., 2021). Furthermore, the IAD was developed by (Ostrom, 2010) while analyzing coordination mechanisms which were novel and still academically unexplored at the time. The same conditions that apply today to governance by blockchain.

First and foremost, the implementation of the IAD framework was useful for truly understanding how governance mechanisms utilized in decentralized exchanges today cannot be categorized as one of the already known institutional regimes. While at the time of writing it holds true that most decentralized exchanges are presenting many elements of corporate governance Davidson (2021), as decision making power centralization, they are presenting at the same time a number of traits and innovations which are unique to them. The different types of voting mechanisms that gauge both time and commitment in governance, and boundary rules are prime examples of such institutional innovation. This once again underlines how new coordination mechanisms are effectively possible by utilizing blockchain as underlying infrastructure.

The application of the vertical approach to the rules in use was in itself also a way to assess how early and underdeveloped the concept of governance in blockchain applications still is. In fact, each of the protocols analyzed has different interpretations of how governance should be. For instance, Curve only allows the community to decide on operational features of the protocol, while the core team is the only one entitled to set constitutional rules. On the other hand, Sushiswap and Uniswap allow the community to also decide on constitutional features (to different extents), such as how the decision making process should take place, and who should hold key positions (in the case of Sushiswap). As a result, even if Curve's voting power were to be more decentralized, in reality key decision making would still be in the hands of the same individuals. Nonetheless, thus far Curve has also been the protocol with the highest total value locked. While on one hand this could be solely attributed to their well designed incentive schemes (payoff rules), it could also signal that given the high technical complexity, it might be wiser to keep key decision making in the hands of few qualified individuals rather than distributing it to a less knowledgeable community of participants having misaligned goals and incentives, at least in these early stages. In this regard, the development of boundary rules able to effectively gauge the true interest and commitment of participants in governance participation is the next logical innovation.

The implementation of the horizontal approach to rules in use analysis revealed that boundary and payoff rules in particular differ the most between protocols. This result coheres with the low exit costs of blockchain applications. Low exit costs allow participant to easily move their capital, time and commitment between projects. As a result, one of the few ways protocols have to retain users is by providing competitive incentives. Again, Curve is perhaps one of the best examples of well designed payoff rules given that it has managed to retain and grow in both users and liquidity consistently over time, despite it being the very first iteration of stable automated market maker design.

The flexibility in defining evaluative criteria also turned out to be an insightful characteristic of the IAD framework. For instance, evaluating the total value locked of the different protocols and their trend over time allowed to assess the impact and relevance of payoff rules. This was clearly visible in the examples of Uniswap and Sushiswap, where the latter was able to attract much of the former's liquidity by simply offering higher rewards. Furthermore, evaluating the involvement of the community and the governance token distribution turned useful in determining that participation in governance is generally quite low and that voting power is fairly decentralized respectively.

Finally, biophysical conditions were perhaps the only building block of the external variables who's implementation turned to be non trivial. Following the theory of Ostrom (2005), biophysical conditions are defined as the attributes of the physical world that affect the variables in the action situation. However, by definition the communities analyzed in this research interact purely in digital settings. As a result, for the purpose of the analysis, biophysical conditions were defined in this case as the attributes of the underlying infrastructure on which the analyzed decentralized exchanges are built, that is the Ethereum blockchain. However, as the industry matures and protocols deploy on multiple blockchains, having different technical characteristics, defining biophysical conditions might become a more thoughtful exercise.

6
Conclusion

Over the last decade blockchain has manifested as a technology able to reduce the costs of transacting value over the internet. By studying its dynamics through the lenses of Institutional Economics, academics have accordingly defined blockchain as an institutional technology (Berg et al., 2019). In particular, following the theories of Williamson (1985), transaction costs associated with bounded rationality, opportunism and asset specificity are the drivers that define contracting processes. As blockchains reduce transaction costs by mitigating opportunism, Berg et al. (2019) have theorized how more transactions would now be possible under 'promise' rather than hierarchical organizations, and how this very shift could foster novel institutional regimes previously unfeasible. The purpose of the following research was to characterize the governance mechanisms of three different decentralized exchange applications running on the Ethereum blockchain, and to determine whether these effectively present and utilize innovative institutional structures.

In order to fulfill the objective of the research, the main research question posed was *'What institutional innovations does blockchain technology introduce to the exchange of financial assets?'*. The methodology utilized to answer this question was the Institutional Analysis and Development framework developed by Ostrom (2010). This particular framework was chosen given its versatility and its institutionally unbiased approach towards the analysis of diverse governance mechanisms, since until this moment in time the governance of blockchain applications has been analyzed solely by comparison with existing and well known institutions (Allen et al., 2021).

The first step towards the characterization of blockchain governance mechanisms was to understand how decentralized exchange applications effectively reduce the costs of transacting financial products as securities. From this the first sub research question was formulated as *'How do decentralized exchanges effectively reduce transaction costs?'*. Decentralized exchanges are a solution to the cumbersome market infrastructure currently coordinating the exchange of financial products. As a matter of fact, multiple firms are necessary for the exchange of securities. Exchanges match buyers and sellers, clearing houses assume counterparty risk and make sure trading parties can meet their obligations, and custodians and central security depositories are responsible for the final settlement of the transaction. Given that fundamentally public and permissionless blockchains are an immutable and censorship resistant record of transactions, they undermine the economic efficiency of traditional clearing and settlement processes by being able to provide instant verification and on chain settlements. Furthermore, it also reduces reconciliation costs therefore further driving down the operational costs of firms involved in the post trade process.

The decentralized exchanges selected for the analysis were Uniswap, Sushiswap and Curve. The criteria that led to the selection of these three included: blockchain of launch, time in the market, total value locked, trading volume and user base. Since the IAD framework relies on large amounts of empirical data, a number of data gathering techniques were utilized to collect all the data necessary to perform the analysis. However, while (Ostrom, 2010) analyzed physically located communities, the communities analyzed in the following research interacted in purely digital settings. As a result, one of the challenges encountered lied in the data gathering methodology itself. This led to the formulation of the second sub research question: *'How and what data can be retrieved for implementing the Institutional Analysis and Development framework?'*. Since Ethereum is a public blockchain, data concerning the activity of the selected decentralized exchanges was retrievable through a number of on chain analytics platforms as Dune analytics and Tally. Data collected from these platforms included total value locked, trading activity, user base and governance token distribution. Furthermore, in order to assess community involvement and governance participation, active on field research was conducted on the relative online forums and voting platforms utilized by the different communities.

The behaviour of the communities and the performance of the protocols were then assessed by analyzing the data in terms of five different evaluative criteria defined a priori. From this the third sub research question was formulated: *'How are evaluative criteria defined and why?'*. The first two criteria outlined were the ones of total value locked and trading volume. While the former is a measure of the amount of liquidity a protocol has been able to attract, the latter provides a measure of the actual utilization of the protocol. The third criteria defined was community size, or how large the user base has grown over time. As presented, each community has experienced a quasi monotonic growth in amount of new participants. The fourth criteria was community involvement, that aimed at measuring how many of the users of the protocol actually participate in governance. The fifth and last evaluative criteria defined was token distribution, that served as a measure of voting power concentration in the different communities by assessing the governance token accumulation of participants.

Addressing the three sub research questions discussed above aided the process of setting up the IAD framework correctly and consequently answer the main research question *'What institutional innovations does blockchain technology introduce to the exchange of financial assets?'*.

One of the first characteristics conveyed was that of all the external variables, payoff rules and boundary rules are the ones that impact and modify the most the behaviour of the community and the performance of the protocol. In particular, a careful and well designed payoff rule mechanism, or in this case incentive schemes, can significantly influence the degree of failure or success of certain protocols over others. In fact, the protocol having the best incentive schemes for both traders and liquidity providers, Curve, is also the one with the largest total value locked by a significant margin. These particular results should not be surprising given the digital conditions on which these protocols are built. Users interact through online applications from different parts of the world and, in most cases, in complete anonymity. Moreover, exit costs are extremely low. Therefore, one of the main institutional innovations concerns the incentives developed by protocols for governance participants and communities at large to behave as desired. In fact, since there is no way in which protocols can enforce users to perform certain actions, the only viable solution to effectively shape their behaviour is to create strong incentives and deterrent.

The analysis also showed that by adopting the vertical approach to rule analysis, different protocols allow for different levels of community participation in governance. In particular, Curve only allows the community to have a say in collective choice governance rules. Meaning, the community can only vote on operational features of the protocol as the deployment of new liquidity pools or the change in certain protocol parameters. Therefore, the community cannot decide on how the decision making process should be or who should be in the core team. On the other hand, Uniswap and Sushiswap have allowed the community to participate in constitutional level decision making, even if at different extents. On one side, Uniswap - having perhaps the least vibrant community - has seen proposals pass as changes to the quorum thresholds. On the other, the community of Sushiswap - being the most vibrant amongst the three - has already voted more than once even on replacement of the management and other key members. This proves that to date, there is no consistent approach and understanding of governance structuring in decentralized exchange applications.

So far, each protocol has tried to distribute voting rights to the community by distributing governance tokens. However, this mechanism has presented a series of drawbacks. Most protocols utilize a one token one vote system, as a result wealthy individuals that manage to accumulate large amounts of tokens consequently have considerable voting power. All the protocols analyzed presented a high degree of token concentration, meaning decision making power is often aggregated in the hands of a few wealthy actors which, in many cases, are usually core team members or early venture capital investors. Last but certainly not least, perhaps the biggest innovation characterizing these new coordination mechanisms allowed by blockchains are the different voting mechanisms. The best example of this is the voting system implemented by Curve, where participants commit both tokens and time in order to gain voting power.

In conclusion, following the results obtained from the analysis the fourth and final sub research question could be answered. It being, *'In virtue of Institutional Economics theories, has the reduction in transaction costs associated with financial exchanges actually modified their governance structure?'*. While one of the claims of the blockchain space has been to be able do decentralize governance, the analysis conducted in this research has proven that, for the time being the governance of decentralized exchanges is resembling hierarchical coordination systems as corporate governance. However, there are signs that suggest new means of coordination are arising. For instance the institutional innovations introduced by new voting mechanisms and boundary rules. Nonetheless, these are still at early stage and it will take some time for radically new institutional regimes to manifest. In sum, the reduction of transaction costs introduced by blockchains are effectively creating new coordination mechanisms as theorized by Williamson (1985), it is just too early for it to be apparent to all analysts.

With all this being said, future work recommendations are to utilize the Institutional Analysis and Development framework to analyze projects in the future having governance at a more advanced stage of development. In particular, close attention should be given to their voting mechanisms, token distribution and payoff rules. As these could be the keys to truly understand the extent to which new institutional regimes are forming. To note that this type of analysis should also be conducted on projects other than decentralized exchanges. Good candidates could be decentralized lending markets and derivative protocols. As the space matures and more participants start to join the space, new waves of technical and institutional innovation will arise, it will be the job of future analysts and academics to analyze these with a consistent and institutional agnostic methodology in order to deeply understand their achievable impact.

Bibliography

Adams, H. (2019). A short history of uniswap. *Uniswap blog*. Retreived from `https://uniswap.org/blog/uniswap-history`.

Aigner, A. A. and Dhaliwal, G. (2021). Uniswap: Impermanent loss and risk profile of a liquidity provider. *arXiv preprint arXiv:2106.14404*. Retrieved from `https://arxiv.org/abs/2106.14404`.

Aite, G. (2014). Reconciliation technology solutions in 2014: Recs get ready to rumble. *Aite Novarica*. Retreived from `https://aite-novarica.com/report/reconciliation-technology-solutions-2014-recs-get-ready-rumble-\global\let\T1\textellipsis.\kern\fontdimen3\font.\kern\fontdimen3\font.\kern\fontdimen3\font\T1\textellipsis`.

Allen, D., Berg, C., Davidson, S., MacDonald, T., and Potts, J. (2021). Building a grammar of blockchain governance. *Crypto Economics*. Retrieved from `https://medium.com/cryptoeconomics-australia/building-a-grammar-of-blockchain-governance-c2cb4b70f915`.

Allen, D. W. (2019). Governing the entrepreneurial discovery of blockchain applications. *Journal of Entrepreneurship and Public Policy*.

Allen, D. W. and Berg, C. (2020). Blockchain governance: What we can learn from the economics of corporate governance. *The Journal of the British Blockchain Association*. Available at SSRN: https://ssrn.com/abstract=3519564 or http://dx.doi.org/10.2139/ssrn.3519564.

Allen, D. W., Berg, C., and Lane, A. M. (2019). *Cryptodemocracy: How Blockchain Can Radically Expand Democratic Choice*. Rowman & Littlefield.

Amini, H., Filipović, D., and Minca, A. (2015). Systemic risk and central clearing counterparty design. *Swiss Finance Institute Research Paper*. Available at `https://ssrn.com/abstract=2275376`.

Auer, R. and Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review, March*.

Bali, T. G., Demirtas, K. O., Levy, H., and Wolf, A. (2009). Bonds versus stocks: Investors' age and risk taking. *Journal of Monetary Economics*, 56(6):817–830.

Bartoletti, M., Chiang, J. H.-y., and Lluch-Lafuente, A. (2021). A theory of automated market makers in defi. In *International Conference on Coordination Languages and Models*, pages 168–187. Springer.

Ben-David, I., Palvia, A., and Spatt, C. (2017). Banks' internal capital markets and deposit rates. *Journal of Financial and Quantitative Analysis*, 52(5):1797–1826.

Berg, C., Davidson, S., and Potts, J. (2019). *Understanding the blockchain economy: An introduction to institutional cryptoeconomics*. Edward Elgar Publishing.

Berg, C., Davidson, S., and Potts, J. (2020). Commitment voting: a mechanism for intensity of preference revelation and long-term commitment in blockchain governance. *SSRN 3742435*. Available at SSRN: https://ssrn.com/abstract=3742435.

Bulat, R. (2018). Uniswap: Understanding the decentralized ethereum exchange. *Medium*. Retrieved from https://medium.com/block-journal/uniswap-understanding-the-decentralised-ethereum-exchange-5ee5d7878996.

Bushman, R. M. (2016). Transparency, accounting discretion, and bank stability. *Economic Policy Review, Issue Aug*, pages 129–149.

Buterin, V. (2014a). Daos are not scary, part 1: Self-enforcing contracts and factum law. *Bitcoin Magazine*. Retrieved from https://blog.ethereum.org/2014/02/24/daos-are-not-scary-part-1-self-enforcing-contracts-and-factum-law/.

Buterin, V. (2014b). Daos, dacs, das and more: An incomplete terminology guide. *Ethereum Foundation Blog*. Retrieved from https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

Buterin, V. (2014c). Welcome to the new beginning. *Bitcoin Forum*. Retreived from https://bitcointalk.org/index.php?topic=428589.0.

Buterin, V. (2017). On path independence. *Vitalik Buterin's website*. Retreived from https://vitalik.ca/general/2017/06/22/marketmakers.html.

Buterin, V. (2018). Governance, part 2: Plutocracy is still bad. *Vitalik Buterin's website*. Retreived from https://vitalik.ca/general/2018/03/28/plutocracy.html.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37). Retrieved from https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf.

Calvão, F. (2019). Crypto-miners: Digital labor and the power of blockchain technology. *Economic Anthropology*, 6(1):123–134.

Capece, G., Levialdi Ghiron, N., and Pasquale, F. (2020). Blockchain technology: Redefining trust for digital certificates. *Sustainability*, 12(21):8952.

Casey, M., Crane, J., Gensler, G., Johnson, S., and Narula, N. (2018). The impact of blockchain technology on finance: A catalyst for change. *ICMB, International Center for Monetary and Banking Studies*.

Cetorelli, N. and Peristiani, S. (2012). The role of banks in asset securitization. *Federal Reserve Bank of New York Economic Policy Review*, 18(2):47–64.

Chamorro-Courtland, C. (2010). Counterparty substitution in central counterparty (ccp) systems. *Banking Finance Law Review 517*.

Chen, Y. and Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13:e00151.

Chitra, T., Angeris, G., Evans, A., and Kao, H.-T. (2021). A note on borrowing constant function market maker shares. *Stanford.edu*. Retrieved from https://web.stanford.edu/~guillean/papers/cfmm-lending.pdf.

Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. *SSRN 3082055*. Available at SSRN: https://ssrn.com/abstract=3082055.

Chuen, D. L. K. (2015). *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press.

Coase, R. (1960). The problem of social costs. *The journal of Law and Economics, University of Virginia*, 3:1–44.

Coase, R. H. (1937). *The nature of the firm*, pages 386–405. Economica.

Collomb, A. and Sok, K. (2016). Blockchain/distributed ledger technology (dlt): What impact on the financial sector? *Digiworld Economic Journal*.

Davidson, S. (2021). From corporate governance to crypto-governance. *Available at SSRN 3844304*.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, 19(5):92–95.

Egorov, M. (2019a). Curve dao. Retrieved from https://curve.fi/files/CurveDAO.pdf.

Egorov, M. (2019b). Stableswap - efficient mechanism for stablecoin liquidity. Retrieved from https://curve.fi/files/stableswap-paper.pdf.

Eichholz, L. (2020). The uni token: Is uniswap really decentralized? *Glassnode Insights*. Retrieved from https://insights.glassnode.com/uni-token-is-uniswap-really-decentralized/.

Emmett, J. (2019). Conviction voting: A novel continuous decision making alternative to governance. *Giveth*. Retreived from medium.com/giveth/conviction-voting-a-novel-continuous-decision-making-alternative-to-governance.

Floor, T. (2020). Benefits of a ccp. *CCP12 Bi-annual newsletter*. Retreived from https://ccp12.org/benefits/.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. In *Qualitative Inquiry*, volume 12, pages 219–245. Sage publications Sage CA: Thousand Oaks, CA.

Froewis, M., Sridhar, K., Makridis, C., and Böhme, R. (2021). The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Available at SSRN*.

Harris, L. (2003). *Trading and exchanges: Market microstructure for practitioners*. OUP USA.

Hashed (2020). Synthetix: the most progressive experiment on the synthetic token and the protocol economy. *Medium*. Retrieved from https://medium.com/hashed-official/synthetix-the-most-progressive-experiment-on-the-synthetic-token.

Hayek, F. A. (1945). *The use of knowledge in society*, volume 35, pages 519–530. The American economic review.

Hendrikx, F., Bubendorfer, K., and Chard, R. (2015). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, 75:184–197.

Hobbes, T. (1904). *Leviathan: or, the matter, forme and power of commonwealth, ecclesiasticall and civill.* University Press.

Holden, C. W., Jacobsen, S. E., and Subrahmanyam, A. (2014). The empirical analysis of liquidity. *Foundations and Trends in Finance*, 8:263–365.

Jakub (21-08-2020). What is impermanent loss? defi explained. *Finematics.* Retreived from `https://finematics.com/impermanent-loss-explained/`.

Jensen, J. R., von Wachter, V., and Ross, O. (2021). An introduction to decentralized finance (defi). *Complex Systems Informatics and Modeling Quarterly*, pages 46–54.

Jensen, M. C. (1986). *Agency costs of free cash flow, corporate finance, and takeovers*, volume 76, pages 323–329. The American economic review.

Joseph, S. (2019). The state of diversity and inclusion in blockchain. *Crowell moring.* Retreived from `https://diversityinblockchain.com`.

Ketokivi, M. and Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, 32(5):232–240.

Kiesling, L. (2019). Transaction costs, the knowledge problem, and the digitalization of the distribution grid. *Engineering and public policy, Carnegie Mellon University.*

Lal, R. and Johnson, S. (2018). Maersk: Betting on blockchain. *Harvard Business School Case.* Retrieved from `https://www.hbs.edu/faculty/Pages/item.aspx?num=54373`.

Lam, W. F. et al. (1998). *Governing irrigation systems in Nepal: institutions, infrastructure, and collective action.* Institute for Contemporary Studies.

Lees, F. A. (2012). *Financial exchanges: A comparative approach.* Routledge.

Liu, L. and Xie, G. (02-11-2021). A mathematical view of automated market maker (amm) algorithms and its future. *Medium.* Retreived from `https://medium.com/anchordao-lab/automated-market-maker-amm-algorithms-and-its-future-f2d5e6cc624a`.

Lo, A. W. and Wang, J. (2000). Trading volume: definitions, data analysis, and implications of portfolio theory. *The Review of Financial Studies, Oxford University Press*, 13(2):257–300.

Loader, D. (2019). *Clearing, settlement and custody.* Butterworth-Heinemann.

Lubin, J. (2014). What is ethereum? project, platform, fuel, stack. *Ethetereum Foundation Blog.* Retrieved from `https://blog.ethereum.org/2014/05/14/what-is-ethereum-project-platform-fuel-stack/`.

Lui, S. S. and Ngo, H.-y. (2004). The role of trust and contractual safeguards on cooperation in non-equity alliances. *Journal of management*, 30(4):471–485.

MacDonald, T. J., Allen, D. W., and Potts, J. (2016). Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. In *Banking beyond banks and money*, pages 279–296. Springer.

MakerDAO (2018). The maker protocol: Makerdao's multi-collateral dai (mcd) system. *Maker Dao Community*. Available at https://makerdao.com/whitepaper/White%20Paper%20-The%20Maker%20Protocol_%20MakerDAO\T1\textquoterights%20Multi-Collateral%20Dai%20(MCD)%20System-FINAL-%20021720.pdf.

Martinelli, F. (16-03-2020). 80/20 balancer pools. *Medium*. Retreived from https://medium.com/balancer-protocol/80-20-balancer-pools-ad7fed816c8d.

May, T. (1988). The crypto anarchist manifesto. *MIT CSAIL*. Retreived from https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

McBride, C. (2015). Turing-completeness totally free. In *International Conference on Mathematics of Program Construction*, pages 257–275. Springer.

Menkveld, A. J. and Vuillemey, G. (2020). The economics of central clearing. *Annual Review of Financial Economics*, 13.

Merkle, R. (2016). Daos, democracy and governance. *Cryonics Magazine*, 37(4):28–40.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Whitepaper.

Narayan, P. K., Mishra, S., and Narayan, S. (2015). New empirical evidence on the bid-ask spread. *Applied Economics*, 47(42):4484–4500.

Nomi, C. (2020). The sushiswap project. *Medium*. Retreived from https://medium.com/sushiswap-org/the-sushiswap-project-8716c429cee1.

O'Shea, V. and Camerinelli, E. (2013). Sibos 2013: One thousand and one reflections. *AiteNovarica report summary*. Retreived from https://aite-novarica.com/report/sibos-2013-one-thousand-and-one-reflections.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge university press.

Ostrom, E. (2005). *Understanding institutional diversity Princeton University press*, pages 393–432. Princeton University press.

Ostrom, E. (2010). Beyond markets and states: polycentric governance of complex economic systems. *American economic review*, 100(3):641–72.

Ozili, P. K. (2022). Central bank digital currency research around the world: a review of literature. *Journal of Money Laundering Control*.

Perucchini, A. (2017). Disrupting finance: who has to beware of blockchain? *Julius Bar*. https://www.juliusbaer.com/en/insights/digital-disruption/disrupting-finance-who-has-to-beware-of-blockchain/.

Petram, L. O. et al. (2011). *The world's first stock exchange: How the Amsterdam market for Dutch East India Company shares became a modern securities market, 1602-1700*. PhD thesis, Universiteit van Amsterdam [Host].

Puljiz, M., Begušic, S., and Kostanjcar, Z. (2018). Market microstructure and order book dynamics in cryptocurrency exchanges. In *Crypto Valley Conference on Blockchain Technology*.

Rekt (06-12-2021). Sushiswap scandal. *Rekt news*. Retreived from `https://rekt.news/sushiswap-scandal/`.

Rothstein, B. (2005). *Social traps and the problem of trust*. Cambridge University Press.

Schaefer, G. K. (2008). An economic analysis of the single euro payments area (sepa). Technical report, FIW Working Paper.

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

Schueffel, P. (2021). Defi: Decentralized finance-an introduction and overview. *Journal of Innovation Management*, 9(3):I–XI.

Shleifer, A. and Vishny, R. W. (1997). A survey of corporate governance. *The journal of finance*, 52(2):737–783.

Stepanova, V. and Eriņš, I. (2021). Review of decentralized finance applications and their total value locked. *TEM Journal*, 10(1):327–333.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First monday*. Available at `https://doi.org/10.5210/fm.v2i9.548`.

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*, volume 3. Random House Incorporated.

Tasca, P. and Tessone, C. J. (2017). Taxonomy of blockchain technologies. principles of identification and classification. *arXiv preprint arXiv:1708.04872*.

Tian, Y., Lu, Z., Adriaens, P., Minchin, R. E., Caithness, A., and Woo, J. (2020). Finance infrastructure through blockchain-based tokenization. *Frontiers of Engineering Management*, 7(4):485–499.

Uniswap, T. (2020). Introducing uni. *Uniswap Blog*. Retrieved from `https://uniswap.org/blog/uni/`.

Walsham, G. (1995). Interpretive case studies in is research: nature and method. *European Journal of information systems*, 4(2):74–81.

Wang, Y. (2020). Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*.

Watch, C. (2021). How to use crytowatch. *Cryptowatch Guides*. Retreived from `https://guides.cryptowat.ch`.

Williamson, O. (1979). Transaction-cost economics: the governance of contractual relations. *The journal of Law and Economics, The University of Chicago Law School*, 22(2):233–261.

Williamson, O. (1985). *The Economic Institutions of Capitalism*. Free Press.

Williamson, O. E. (1981). The economics of organization: The transaction cost approach. *American journal of sociology*, 87(3):548–577.

Williamson, O. E. (1996). *The mechanisms of governance.* Oxford University Press.

Wright Jr, D. (2019). Quadratic voting and blockchain governance. *Heinonline.* Retreived from https://heinonline.org/HOL/LandingPage?handle=hein.journals/umkc88&div=22&id=&page=.

Wyman, O. (2015). The capital markets industry. *Swift.* Retreived from https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2015/March/The_Capital_Markets_Industry.pdf.

Yin, R. K. et al. (2003). Design and methods. *Case study research*, 3(9.2).

Younessi, C. (04-12-2018). Uniswap — a unique exchange. *Medium.* Retreived from https://medium.com/scalar-capital/uniswap-a-unique-exchange-f4ef44f807bf.

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., and Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105:475–491.