Hello everyone!

In this post, I shall attempt to delineate and present some musings on decentralisation. Given the Protocol's collective aim to progressively decentralise, I thought that providing insight as to what this actually entails would be beneficial so as to make sure that the Community has an adequate understanding of the principles underpinning this concept.

By way of an introduction to those that do not know me yet, I am Immutablelawyer

. I have been actively contributing within the dYdX Ecosystem for the past six months in areas relating to law, decentralisation and governance. By way of background, I am a Senior Legal Analyst with a crypto-focused consultancy firm and have been working in the industry for the past 3 years now. We provide a myriad of services including Token Classification Reports, Decentralisation & Legal Risk Audits and Advisory services in relation to numerous areas such as: DeFi product structuring (technical and legal back-end structuring), progressive decentralisation, jurisdictional setups, tokenomics, intellectual property etc. We also actively work with exchanges of a centralised and decentralised nature and advise them on a myriad of technical and regulatory matters. Throughout my career, i've provided clients with advice in relation to jurisdictions such as Guernsey, the Cayman Islands, the British Virgin Islands, Switzerland, Liechtenstein, Bermuda, the United States, Malta, Singapore, and other European Union member states. Naturally, having to study regulatory frameworks within a vast number of jurisdictions leads one to gain a certain level of understanding in relation to structures which could be used to support certain Protocols within the space and jurisdictions which would not be adequate to set up certain key functions of an Ecosystem.

Now, let's get to the crux of the matter - decentralisation. Decentralisation has been a prominent buzzword used by many within the industry for the past few years. This buzzword has been most notably used in conjunction with the 'DAO' acronym, ergo, a 'Decentralised Autonomous Organisation'. By way of a history lesson on this DAO nomenclature, DAOs were initially referred to as DACs in 2013 by Stan Liemer, Dan Liemer and Vitalik Buterin i.e. Decentralised Autonomous Corporations' (you can find Vitalik's article discussing DACs on Bitcoin Magazine here: https://bitcoinmagazine.com/technical/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274) (you can find Stan's resources on DACs here Bitcoin and the Three Laws of Robotics — Steemit).

Stan and Dan Liemer had previously made reference to the three laws of robotics which he deemed to be essential pre-requisites in having a DAC. Without the presence of these laws of robotics, you essentially have no Robot. These laws of robotics are the following:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

However, these were then moulded to be used and implemented in the case of DACs and Dan and Stan Liemer came out with the following adapted rules of robotics to DACs:

- A DAC must always obey its own published business rules.
- A DAC must never change its rules without consent of its stakeholders, except where such change would conflict with the First Law.
- A DAC must protect its own existence, as long as such protection does not conflict with the first two laws.

What is a DAO?

Following that brief history lesson (the details of which have been re-birthed in Gabriel Shapiro's paper on BORGs), we will now move onto DAOs. The term DAO has been liberally used by the industry for a while now - it is a keyword, a buzzword, used by various sectors of the community to depict that a particular protocol is community-driven, community-led and community-controlled. However, when you look under the hood, most protocols are anything but decentralised, autonomous, or organised.

The term DAO should be looked at as a test rather than as a classification. The first pre-requisite is Decentralisation (the primary pre-requisite that will be tackled in today's post). Decentralisation is not a term that was created by cypherpunks or the crypto industry. Decentralisation has actually been a topic that has been discussed for decades by entities at the governmental level - wherein decentralisation normally takes the form of selecting functions, rights and obligations which are in one governmental body, and distributing those functions, rights and obligations to numerous other separate governmental bodies. Hence, in practice, decentralisation at the government-level is efficiency-seeking in nature - yet, the underlying intention is always the same (even in our industry).

Hence, to sum up the above, decentralisation is a concept that refers to the distribution of power and decision-making away from a central authority or group - resulting in a system where power and control are distributed among multiple individuals, organisations, or entities, instead of being concentrated in the hands of a few (when this is distributed to multiple entities making up a Protocol's legal back-end, one must make sure that these entities are made up of separate individuals and separate ultimate beneficial controllers/owners. otherwise, you wouldn't have decentralised anything but rather, you would have created multiple entities and maintained the same centralised level). Decentralisation can thus take many forms,

including political, economic, legal and technological. Economic decentralisation for example involves the spread of economic power and resources across different individuals or organisations, rather than being controlled by a few dominant players.

Autonomy refers to the liberal exercise of the same functions, rights and obligations that would have been decentralised as per above. Hence, in the case of a protocol that would have been launched by a private company, autonomy would relate to the rescinding of control over the tech-stack by that private company, to a community of token-holders for that community of token holders to exercise the functions, rights, and obligations that were inherent in such a private company (I will potentially write a separate thread on Autonomy).

Organisation is simple in nature yet has created ambiguity in its achievement. Organisation refers to a set of factors namely, legal organisation and technical organisation. With regard to the legal organisation, one refers to an entity that enables members of a community or a sub-set of that community to conclude agreements for the benefit of the protocol the community operates in relation to (in an autonomous manner - always circling back). However, organisation also refers to methods of communication (forum, discord, etc.), and hierarchical structures that would benefit the assignment of tasks, recruitment of capable members, the filing in of leadership roles by community consent etc. From a technical perspective, organisation refers to voting and proposal mechanisms, off-chain polling and on-chain voting, on-chain proposal ratification and implementation in an automatic (again circle back to autonomy) manner (refer to compound governance alpha) etc. All in all, a robust governance structure is a good sign of a certain level of organisation (this needs to be coupled with the aforementioned factors as well which are but some mentions of the factors that need to be in place).

How do we interpret decentralisation in WEB3 though? Well, this is where it gets very interesting. Decentralisation in on-chain financial service providers/protocols (as is the case with dYdX being an on-chain financial service provider re. crypto derivatives), mainly relates to the following:

Technological Decentralisation.

Technological decentralisation primarily relates to the rescinding of code-level control over a particular tech-stack. In the case of a protocol like dYdX, the most important step towards achieving a substantial level of technological decentralisation is the sacrificial (this is dramatic) burning of the Admin Keys. Burning Admin Keys refers to the intentional destruction of the private keys that grant administrative access to a blockchain network or protocol-level tech-stack. Admin Keys grant special privileges, such as the ability to modify the software at will, upgrade the software, or even destroy the software altogether. Without burning Admin Keys, a protocol or a blockchain always runs the risk of having this single point of failure being used maliciously or otherwise, or falling into the wrong hands. Burning admin keys is often done during the launch of a new blockchain network or during a major upgrade, as a way to ensure that the network remains truly decentralised and resistant to centralised control or manipulation. However, it is important to note that burning admin keys can be a controversial decision, as it may limit the ability of the network to respond quickly to emergencies or to make necessary quick upgrades in the future. However, as we all know, decentralisation does have its pitfalls - the main one being less efficiency in decision making.

Other steps towards technological decentralisation differ on a case by case basis. In the case of a tech-stack using validator nodes to reach consensus/perform certain functions, technical decentralisation is achieved by substantially increasing node count, reducing the barrier to entry to operating nodes (which in turn increases node count), ensuring that there is a sufficient incentivisation framework in place to support multiple software developers to improve the protocol at a time (instead of having one software developer maintaining the protocol) and ensuring that the particular product, protocol, or blockchain has multiple front-ends so that it always has an access-point to be used by the end-user.

Economic Decentralisation

Economic decentralisation relates to the distribution of incentives by a particular blockchain or protocol built on such protocol. Miles Jennings does a great job of entering into detail and providing examples of achieving this economic decentralisation in his paper titled ‘Principles and Models of Web3 Decentralisation’. By way of an example, we currently note that 40% of current dYdX Trading Rewards are currently accumulated by one account holder (refer to Revitalising the dYdX Rewards System: Innovative Strategies for Enhanced User Adoption, Platform Growth, and Increased Trading Volume). Hence, here, we have a problem of economic centralisation which could leak into other facets of the protocol and lead to centralisation in those other facets (decentralisation and centralisation both have a domino effect when present). In the aforementioned paper, Miles provides a clear example of economic decentralisation which I will cite below:

“for a decentralized economy to function, it needs to properly balance the distribution of the value it accrues (e.g., information, economic value, voting power, etc.) to its stakeholders (developers, buyers and sellers). Any significant and sustained imbalance in this arrangement may jeopardize the system’s economy. For instance, because the native governance token is utilized as an incentive mechanism in the functioning of the system’s economy, an imbalance in the accrual of information relevant to the value of the native governance token (such as information relating to the functioning of the marketplace) could enable a party to manipulate the market for their own benefit. Similarly, an imbalance in the accrual of voting power could enable a party to change the rules of the marketplace for their own benefit. Finally, if the economic value the marketplace accrues is not equitably distributed among its stakeholders, a disfavored constituency may depart for other competitive marketplaces. While the decentralized economy of the marketplace may survive isolated imbalances in the short term (particularly if they advantage benevolent actors), in the long term these imbalances would ideally be removed to prevent them from being exploited.”

Conclusion

That’s enough for today. I did not enter into the regulatory elements as that would necessitate a different post altogether which would build upon this one. The above is very high-level in nature

and was drafted in just 15 minutes. However, considering the discombobulated interpretation of DAOs and decentralisation within the community, I thought that providing a guiding light in relation to what decentralisation is would be beneficial in spearheading efforts to eventually achieve it.

As I stated above, decentralisation and centralisation have proven to be domino effects. If decentralisation is achieved in an organised manner, then you would have automatically created a certain level of autonomy to build off of. A satirical way of looking at it is that achieving decentralisation is a game of whack-a-mole, with the moles being Single-Points-Of-Failure/Pockets of Centralisation.

I hope you found the above interesting - feel free to discuss below!