

Sufficient Decentralization: A Playbook for web3 Builders and Lawyers

By [Marc Boiron](#), Chief Legal Officer at dYdX Trading¹

Introduction

Web3 builders have focused on the concept of “sufficient decentralization” ever since staff at the U.S. Securities and Exchange Commission introduced the concept in 2018. It led builders to focus on distributing the efforts of driving profits in a crypto-asset from a centralized company to unaffiliated community members working towards a common goal.

Given that blockchains are nascent *technologies*, most legal advice around securities laws focuses on decentralizing the web3 technology stack. But just as important is to decentralize the off-chain, day-to-day activities of community contributors. This work, none of which takes place on a blockchain, includes developing the protocol or software around the protocol, engaging in business development, marketing and growing the protocol, making intellectual property available for all to use and advancing protocol governance.

Yet these contributions, which this playbook defines as off-chain activities, are difficult to automate and can increase bureaucracy, meaning off-chain activities around decentralized protocols tend to gravitate toward centralization. To achieve robust decentralization, communities have to be intentional about how they structure both on and off-chain activities.

This playbook is for (1) web3 founders who want to efficiently decentralize off-chain activities while remaining compliant with U.S. securities laws and (2) web3 lawyers advising those founders. It explains what “sufficient decentralization” means, how it affects off-chain activities, common errors that lead to the centralization of decentralized autonomous organizations (DAOs) and how to efficiently structure a community to achieve “sufficient decentralization.”

Although this playbook provides a view on how to efficiently decentralize off-chain activities, it is not intended to imply that the methods contemplated in it are the only ways to do so. There is no single, canonical definition of sufficient decentralization, nor is there a perfect way to achieve it. Certain approaches that companies and communities have taken to date may offer alternatives, and in some cases, alternative approaches may even be more conservative from a regulatory perspective even though they may be less efficient.

¹ Special thanks to Miles Jennings, Rebecca Rettig, Rob Stevens, and Joshua Watts for their significant contributions.

Investment contracts: a primer

In the U.S., a securities issuer has to register a securities offering with the SEC, or rely on an exemption. When registering, the issuer must disclose significant information about the business, the market and the securities offering. These disclosures are designed to protect investors by sharing information that reasonable investors would want to know. It also creates a “level playing field” by preventing any party, including the issuer, from knowing more important information than anyone else.

One type of security that triggers registration obligations is an “investment contract.” To determine whether a contract, scheme or transaction² constitutes an investment contract, the courts have relied on the “*Howey test*,” a four-pronged analysis that the U.S. Supreme Court devised in the 1946 case, *SEC v. W.J. Howey Co.* The Supreme Court concluded that an investment contract is where the transaction (1) involves an investment of money (2) in a common enterprise (3) with a reasonable expectation of profit (4) solely based upon the efforts of others. Courts later interpreted the fourth prong to mean that the reasonable expectation of profits is derived primarily from the entrepreneurial or managerial efforts of others. All four prongs must be met for the given transaction to be deemed an investment contract. That test remains in place today and is used to determine whether the sale of crypto-assets constitutes the sale of an investment contract.³

Crucial to the analysis of an investment contract is whether investors expect a profit from someone else’s entrepreneurial or managerial efforts under the fourth prong of *Howey*. Accordingly, a key determinant of whether the sale of a crypto-asset is also an investment contract is whether people could reasonably expect that web3 contributors drive the value of a cryptocurrency, including through off-chain activities.

What does sufficient decentralization mean?

The idea of “sufficient decentralization” was introduced in a June 2018 speech by William Hinman, who at the time was the director of the SEC’s Division of Corporation Finance. Hinman [said](#): “If the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract.” With that framework in mind, Hinman concluded that *current* sales of Ether were not sales of securities because the Ethereum network had become sufficiently decentralized.

² For the sake of simplicity, this playbook uses the terms contract, scheme and transaction interchangeably.

³ This playbook refers to crypto-assets as investment contracts (and, thus, as securities) for simplicity. In reality, crypto-assets may form part of an investment contract but are not themselves the investment contract. Put another way, the issuer of the investment contract makes certain promises (whether implied or express and whether in writing, oral or through actions) that causes purchasers of crypto-assets to expect a profit; those promises wrap the crypto-asset to form the investment contract but do not become part of the crypto-asset. So, when this playbook explains that crypto-assets can transform from securities to non-securities, those explanations should be understood as references to the investment contract falling away rather than the transformation of the underlying crypto-asset.



“If the network on which the token or coin is to function is **sufficiently decentralized** – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may **not** represent an investment contract.

— WILLIAM HINMAN
FORMER DIRECTOR OF SEC'S DIVISION OF CORPORATION FINANCE

Hinman’s “sufficient decentralization” concept was a nod to the last prong of the *Howey* test, which assesses whose efforts drive the purchasers’ expectations of profit in a crypto-asset. If a protocol or network⁴ is not sufficiently decentralized, then the value of the associated crypto-asset can be derived from the efforts of a centralized team – a person, or a group of people, who the public believes coordinates to increase the value of a crypto-asset. And if the protocol *is* sufficiently decentralized, then the value of the associated crypto-asset does not derive from what the public believes to be a centralized team’s efforts – no identifiable, coordinated group drives the value of the crypto-asset.⁵

⁴ This playbook refers to protocols and networks interchangeably based on the understanding that either one of them may be associated with a crypto-asset that accrues value in a sufficiently decentralized manner.

⁵ This playbook focuses on how to avoid the existence of “efforts of others” under the *Howey* test through sufficient decentralization. However, an underexplored means of avoiding “efforts of others” under the *Howey* test is to consider the efforts of holders of crypto-assets themselves. This is similar to how interests in limited liability companies often are not securities because holders could expect to derive profits from their own efforts, even if they do not actually engage in day-to-day activities. Despite differences across U.S. courts, three factors usually determine the existence of an investment contract under this theory: (1) the investor is so powerless that all power is distributed in the way it would be in a limited partnership, where the limited partners rely entirely on the general partner to make decisions; (2) the investor is so inexperienced and unknowledgeable in the enterprise’s business affairs that the investor cannot intelligently exercise powers; and (3) the investor depends so much on someone’s unique entrepreneurial or managerial abilities that the investor cannot replace that other person or meaningfully exercise power. In a typical web3 governance system, where the software code is open-source and no centralized company exercises trademark rights, holders of crypto-assets have significant power to run the business, for instance by altering and marketing the protocol. Many holders will have sufficient experience or knowledge to meaningfully contribute to growing the protocol, and, except in limited cases, will not depend on the unique abilities of someone else, such as the initial development team, to exercise their powers. If so, it would not matter whether an uncoordinated group of third parties creates value for holders of crypto-assets, because holders could engage in activity relating to the protocol that would

The SEC’s Strategic Hub for Innovation and Financial Technology (better known as FinHub) solidified the concept of sufficient decentralization in April 2019 through its “Framework for the Investment Contract Analysis of Digital Assets.” The FinHub framework gave detailed guidance on each prong of the *Howey* test. In doing so, it introduced the idea of an “active participant” as “a promoter, sponsor, or other third party (or affiliated group of third parties)” in relation to the last prong of the *Howey* test.

While the FinHub framework considers an active participant as potentially being an “affiliated group of third parties,” it is possible that, when mentioning affiliates, the framework deviates from the use of the term as defined in SEC regulations and instead is referring to coordinated action among a group of third parties. Unlike an uncoordinated group of third parties working on a protocol, a coordinated group of third parties may have access to significant material information that they would have to disclose under securities laws.

According to the FinHub framework, several factors should be considered when determining “reliance on the efforts of others”—namely whether “essential tasks or responsibilities are expected to be performed by an [active participant], rather than *an unaffiliated, dispersed community of network users*”.

But even if a crypto-asset had originally been sold as an investment contract, the FinHub framework outlines how it could later be sold as a non-security. The asset could mutate (meaning that it eventually would fail to satisfy the *Howey* test) if the entrepreneurial and managerial efforts of an active participant, which could include anyone who later becomes an active participant, no longer continue “to be important to the value of an investment in the digital asset” or “affect[ed] the enterprise’s success.”

In short, if someone reasonably expects to profit from a crypto-asset because of someone else’s entrepreneurial or managerial efforts, including the efforts of active participants, then the sale of that crypto-asset satisfies the final prong of the *Howey* test.⁶ But if that person reasonably expects to profit from the uncoordinated efforts of a broad range of people, that prong should not be satisfied; the protocol and the activities related to it should be considered “sufficiently decentralized” and no investment contract should be deemed to have been sold.

Legal counsel advising web3 participants on distributions or sales of crypto-assets often integrate the concepts of “sufficient decentralization,” “active participants” and mutation. Consequently, well-advised participants have become familiar with seeking to replace the

result in profits and, therefore, theoretically could have an expectation of profits from their own efforts, even if they do not intend to engage in such efforts.

⁶ When the initial development team and community make available publicly all information regarding their current and planned activities supporting the value of a crypto-asset, it may be reasonable to believe that all future purchasers of the crypto-assets could have learned that information when making a decision to purchase the crypto-asset, such that the information may become part of the scheme that may constitute an investment contract. We are not aware of any case law that either supports or rejects this position.

active participants of a centralized protocol with a sufficiently decentralized, uncoordinated group of people who drive value to a protocol.

However, a protocol’s technology and its autonomous operation may not always be the only element that is reasonably expected to drive the value of a given crypto-asset. People who reasonably expect a profit from a crypto-asset could consider additional off-chain activities as value-driving. As a result, to reduce risk to any web3 participants, communities should also seek to decentralize off-chain activities, including, with respect to:

- protocol development
- business development
- growth and marketing
- intellectual property
- governance decisions

The graphic features a dark blue background with white text. At the top left, it reads 'SUFFICIENT DECENTRALIZATION: A PLAYBOOK FOR WEB3 BUILDERS AND LAWYERS BY MARC BOIRON'. The main title 'Off-chain Activities' is prominently displayed in large white font. To the right, a white text block states: 'To reduce risk for all community participants, networks should seek to decentralize their off-chain activities:'. Below this, a list of five activities is presented in white text within light blue rounded rectangular boxes: 'Protocol Development', 'Business Development', 'Growth and Marketing', 'Intellectual Property', and 'Governance Decisions'. A small white pixelated logo is located in the bottom right corner of the graphic.

How off-chain activities may drive a crypto-asset’s value – and thus, whether they influence the outcome of *Howey*’s “efforts of others” test – depends on many factors, including a protocol’s design, target market, and governance mechanism.

For instance, in early-stage protocols, or where protocols that integrate easily with others, community protocol development may have the greatest impact on driving the value of the associated crypto-asset. Conversely, in communities where the protocol design is established, or where integrations are difficult, greater value may be created through business development, growth, marketing, and governance.

What is the spectrum of decentralization?

In web3 communities, there is usually a tension between the efficiency of centralization and the ideological or censorship-resistant allure of decentralization. Each community must balance the desire to benefit from the speed, cost and operational efficiency of centralization against the benefits of decentralization – consensus-building, censorship resistance, transparency, and independence. Communities accept varying levels of centralization and, consequently, fall haphazardly across the “spectrum of decentralization.”

To increase performance and efficiency more centralization is required; to maximize decentralization, some speed must be sacrificed and inefficiencies will exist. Each community will determine with time, either intentionally or not, where on the spectrum of centralization to decentralization its off-chain activities are located. On the centralized side of the spectrum one person or the coordination of one company or small group of people can engage in all off-chain activities. On the decentralized side of the spectrum anybody can participate in any of the off-chain activities at any time without communicating with any other person participating in off-chain activities for the same protocol.

On a technological level, so-called Ethereum killers often achieve faster and cheaper transactions than the Ethereum network at the cost of greater centralization. This is an unacceptable tradeoff for many in the Ethereum community but appropriate for the communities that have made the tradeoff (who also often believe that their protocols will one day be as decentralized as the Ethereum network).

The same tradeoffs apply to off-chain activities. A small group of people coordinating constantly, such as a company, might find it more efficient to centralize off-chain activities. For instance, centralizing marketing operations through one marketing agency is highly efficient because a single marketing manager can direct a hand-selected team to deploy multi-medium marketing campaigns on Discord, Twitter, Telegram and other social channels. Speed and consistent messaging are achieved because one marketing agency controls the access to the protocol’s social channels and the content posted on them..

Conversely, a completely decentralized community might allow anyone to participate in any off-chain activity without communicating with other participants. This is inefficient; to continue the example above, without a manager to coordinate the community’s marketing efforts, anybody could take the initiative to promote it for themselves, no matter their ability to do so – or nobody may market the project at all.

For purposes of the *Howey* test, the more centralized a community, the greater the risk that sales of a crypto-asset are deemed sales of securities.⁷ Yet many other factors impact the degree to which a community decentralizes:

- culture
- historical development of off-chain activity within the community
- censorship risk associated with the community's activity
- leadership within the community
- its strategy for growing use of the protocol
- the coordination necessary to adjust parameters or other aspects of the protocol.

SUFFICIENT DECENTRALIZATION:
A PLAYBOOK FOR WEB3 BUILDERS AND LAWYERS
BY MARC BOIRON

What are the key factors that impact a community's ability to decentralize?

- Culture
- History of off-chain activity
- Censorship risk
- Community Leadership
- Growth strategy
- Coordination necessary to adjust the protocol



Although a web3 community is, by its nature, amorphous, community members can still arrive at a rough consensus about the level of decentralization. The community may even have a de facto “leader,” in the way that Vitalik Buterin is a leader in the Ethereum community, to help

⁷ The term “sales” as used in U.S. securities laws is much broader than the way most people think about it. Under those laws, a transfer of crypto-assets that in any way advances the economic interests of the transferor likely is considered a “sale.” For this reason, even if a person is not transferring crypto-assets in exchange for compensation in the way that people would generally think of crypto-assets being sold, that person should pay attention to whether the crypto-assets may be securities, both due to potential action from the SEC and from a private plaintiff.

reach this consensus. Once achieved, communities should set up processes that protect that level of decentralization and defend them diligently.

Decentralization of a community should take into consideration the sum of all components of the community; communities should accept centralization in areas that might benefit from the increased efficiency it provides and compensate by further decentralizing other off-chain activities. For example, if an early-stage protocol development would benefit from the coordination of a tight-knit group of specialists, then that centralization could potentially be offset if the community decentralizes other off-chain activities.

Many initial development teams and community members consider the impact of their actions and ask whether an action is problematic for decentralization. It is rare that an action will be problematic; instead, all actions in the aggregate should be considered. Whenever anyone engages in activity around a protocol, they either help or hurt decentralization. Thus, the best frame of reference is a continuous evolution of decentralization.



Difficulties with Decentralizing Off-chain Activities

Decentralizing off-chain activities is achievable; doing so efficiently is difficult. This is primarily a communications problem: everyone participating in off-chain activities must be aware of others' work without coordinating so closely that they risk being an "active participant" under the FinHub framework's application of the *Howey* test, causing a crypto-asset to be deemed an investment contract.

Once again, communities must strike a balance between two extremes. Close coordination leads to centralization but chaos would ensue if community members did not share information with other contributors in their community.

For instance, if community marketers only communicated among themselves, then other contributors would not understand how the protocol is marketed. Software developers, for instance, would not be able to understand their users' needs, resulting in software development based on intuition rather than user feedback marketers receive.

Equally, if all community members are in constant, private communications, then they would have centralized the off-chain activities in the same way as a centralized company. Communities working on off-chain activities must avoid forming groups that coordinate a significant portion of the off-chain activities of a protocol. Continuing the example above, the marketing team should provide updates on their activities (such as timelines, status, plans and feedback) on public social-media platforms and governance forums.

Communities need to determine the most practical way of communicating publicly. This requires careful consideration of the appropriate tools. For example, Notion pages can be made public, Zapier can be used to allow anyone to view those public Notion pages and updates can be logged into Linear. In addition, Loom videos can be embedded in public Notion pages, and all Discord channels can be made public.

Community members may be concerned about issues of competition and confidentiality inherent in publishing roadmaps and status updates in public communications channels. However, on most community forums, members openly discuss the future of the protocol and off-chain activities, such that the most sensitive competitive information is already known. In web3, how a community *executes* on competitive information will determine its success, not the confidential information it holds. Where community members who participate in off-chain activities acquire confidential information, they risk obtaining material asymmetric information relative to community members who are not active in those activities, which could strengthen arguments in favor of crypto-assets being treated as securities.

Confidentiality is less of a concern in web3 as most information is not or need not be confidential. The concern still exists for business development or marketing community members who cannot share confidential information they receive from third-parties. In part, this can be addressed by agreeing with third-parties that the relationship or contract is not considered confidential. In that case, community members with confidential information should attempt to provide a generalized description of the circumstances in which the confidential information is being created. When this issue cannot be addressed in that manner, it is incumbent on those community members to ensure that their activities do not create pools of information that are important to crypto-asset holders.

How are off-chain activities decentralized?

Depending on the nature of a crypto-asset, the initial development team's off-chain activities could cause crypto-asset holders to reasonably expect to profit from these efforts. The strategies outlined below reduce this expectation.

When implemented properly, they distribute that expectation across a broader group of people who do not have to coordinate with any other groups. This increases the expectation that crypto-asset holders will profit from the efforts of this broader group, and decreases the expectation that profit will come from the initial development team's efforts, or from those of any other coordinated group.



**SUFFICIENT DECENTRALIZATION:
A PLAYBOOK FOR WEB3 BUILDERS AND LAWYERS
BY MARC BOIRON**

Tips to Decentralize Off-chain Activities

- Software Development:** keep code open source; make the protocol easy to integrate with others
- Business Development:** Give BD team clear direction, financial resources and certainty
- Marketing and Growth:** Use grants and bounties to incentivize growth and marketing; empower independent efforts
- Intellectual Property:** Abandon or distribute IP to the community
- Governance:** Reconsider norms; create code and guides for basic, repeatable proposals



Protocol Development

Although tight-knit teams often initially create protocols, they frequently open up protocol development to a willing community of coders after releasing the protocol. The community might modify the existing code or deploy upgraded versions of the protocol. They also may build software that integrates with the protocol, creating greater demand or different use cases for the protocol.

To effectively decentralize protocol development, all deployed protocol code should be open source. If not, the community cannot continue building the protocol, or software to run on top of it. Since it is highly likely that the protocol's initial developers understand the code better

than anyone else, they should ensure that the code is clean and properly documented. Further, a community should provide robust development and governance guides to reduce barriers to community contributions and knowledge asymmetry. This will allow the community to meaningfully contribute to the code and use the protocol.

Of course, since the initial developers are more familiar with the code than community members, they likely will remain best positioned to develop software that involves the protocol. As such, community developers may not bother modifying or improving the code, hampering the decentralization of protocol development. To incentivize community members to contribute to protocol development, the community can offer grants and bounties.

In the case of grants, the community should identify areas where protocol modifications or improvements are possible, then issue requests for proposals from developers who can build them. While it may be difficult for a community to identify those areas without some guidance, open-source code and public code development should make this easier. That guidance can come from a roadmap published by a product team, the community members, or high-level strategy laid out for the community by the initial development team or other respected community members. Examples of robust grants programs in DeFi are those associated with the [Aave protocol](#), [dYdX protocol](#), and [Uniswap protocol](#). Several layer 1 and layer 2 networks have significant grants programs in the form of funds, such as those associated with the [Polygon network](#) and the [Zcash network](#).

In the case of bounties, the community should ensure it pays valuable contributors.⁸ A formal bounty program helps address this difficulty, as does promoting high-value contributors – think a web3 take on an “employee of the month” scheme. Bounties are more likely to work when contributors become confident that they will be handsomely and consistently rewarded for their efforts.

For grants programs and bounty programs, the application, evaluation, and funding of an initiative should be public. For example, requests for proposals and community driven applications should be available on a community forum; the evaluation and negotiation of objectives, key results and performance indicators should be available for community review; and the completion of a grant and funding of the individual or team should be publicly announced.

Business Development

Business development is the practice of increasing protocol usage by forging targeted, private relationships with third-parties, such as other protocols or institutions. It likely is the most difficult off-chain activity to decentralize after protocol development. This is because business development relies on a small number of personal relationships, where trust is commonly developed in-person.

⁸ This concept is similar to the retroactive public goods funding that Vitalik Buterin [proposed](#).

The following will promote successful community-led business development: (1) a community's business developers should be engaged in the role full-time, (2) communities must provide a clear intention regarding business development goals, (3) business developers must have appropriate financial resources and (4) resources should be clearly demarcated, such that a small group of community members can use them to fulfill commitments to counterparties. This approach likely will prove effective for community members engaging in business development.

To limit the information that any person acquires in a business development role, the business development function can be split across various efforts, such as wallet providers, aggregators, and institutions. This way community members engaged in some but not all of those efforts do not acquire a disproportionate amount of important information regarding value accruing to the protocol.

Due to the personal relationships forged during business development, there is a high risk that those engaged in business development receive material non-public information. One way to address that risk is for communities to approve business development deals in advance, or to subject those deals to community approval. Alternatively, business developers can have a higher amount of discretion if they are transparent with the community and the community has the option to freeze a given business development activity for further community review. These options may make it difficult for business development teams to assure potential partners that transactions will be closed, but it may be necessary at times to safeguard decentralization.

Growth and Marketing

By contrast, growth and marketing are the easiest off-chain activities to decentralize. Although centralized marketing strategies, coordinated by a handful of salaried marketing managers, are ideal, decentralized marketing strategies that rally around a common message can prove highly effective. After all, little coordination – or indeed, knowledge, skill or additional financial incentive – is required to flood Telegram chats with memes or cry “FUD” when criticism is levied at the project.

Four factors contribute to efficient decentralization of growth and marketing activities:

First, code that can easily integrate with other protocols can decentralize growth and marketing. Permissionless protocols allow other protocols to integrate the original protocol without assistance.

The ease with which a protocol can integrate into another is known as composability. Highly composable protocols attract a wide range of users because another protocol can integrate the original protocol without requiring the input of anyone from the original protocol's community.

The integrated protocol can attract integrations from yet more protocols, further growing the original protocol. If these protocols also are decentralized, then their communities can continue to market the original protocol at no extra cost. For instance, when the Aave protocol

was deployed on the Ethereum network, it attracted billions of dollars of crypto-assets without requiring the Ethereum Foundation's help to deploy or market it.

The number of users and volume could grow in lockstep with the number of successful integrations. Even if the integrated protocol is built on multiple protocols, its users' activity will flow through to each protocol with which it is integrated, resulting in partial growth and marketing for each of those protocols. For example, the PoolTogether protocol's integration with the Compound protocol brought thousands of new users to the Compound protocol, promoting the strength of the protocol and driving hundreds of millions of dollars of volume into the Compound protocol.

Protocols also benefit when interfaces and applications build on them. Any users they attract also become users of the protocol, without the protocol's community having to take further action. As an example, the 1inch routing application routes orders to several decentralized exchanges, including the Uniswap protocol, which drives volume to the Uniswap protocol without involvement from Uniswap Labs.

For composability to be most effective, initial development teams should focus on writing clean code with clear documentation and useful tutorials. This will make it easier for others to integrate with the protocol. All code should be licensed under a permissioned open-source license so that other developers can use it.

Second, the community can further decentralize growth and marketing by paying developers through grants and bounties. These grants and bounties can encourage integrations and could entice developers to build tooling for the protocol, such as frontends and block explorers. Grants and bounties can be approached in the manner specified with future protocol development, or they can be automated. For example, the Liquity protocol can automatically [reward](#) developers who operate a front-end interface that integrates its protocol.

Third, grants and bounties can pay for conventional approaches to growth and marketing. Communities can identify the best growth and marketing strategies for acquiring new users, then use grants and bounties to implement growth and marketing campaigns within those channels. The only difference from traditional growth and marketing is that those carrying out these activities are not necessarily affiliated with the protocol, only aligned with its vision and funded by grants or bounties.

Fourth, the community can empower other members to grow and market the protocol on their own time and at their own expense. This allows for greater creativity, since marketers are free to do whatever they want. In addition, as most marketers will be financially invested in the protocol, they do not require additional funds. Bitcoin is an excellent example of effective decentralized marketing. Community members have [sponsored an IndyCar](#) at the Indianapolis 500 and launched [podcasts](#) and [YouTube channels](#) that discuss Bitcoin. This marketing was possible because of the strong community and because each bitcoin holder is incentivized to increase the value of the Bitcoin network.

Intellectual Property

Communities can decentralize intellectual property, including copyrights and trademarks, to prevent a single party from creating value for the community.

A copyright protects original works of authorship, such as code, when the author, such as a developer, puts that work into tangible form, for instance by typing the code. A trademark can include things like the protocol's name, slogan, logo, or a combination of these that identifies a good or service, such as a protocol.

Communities can use trademarks and copyrights offensively or defensively. Defensive uses, like defending against a claim of an infringement of an intellectual property right, rarely create value because they only protect the holder of that property right. Offensive uses, such as preventing others from using the trademark to dilute the value of a brand, usually create value. They protect the protocol associated with the brand and prevent others from using copyrighted code to create a competitive product.

To decentralize intellectual property, a centralized party should abandon all copyrights and trademarks, or transfer them to the community by assigning them to an entity in the community's legal structure. This is complex because the laws governing copyrights and trademarks are inconsistent across jurisdictions but possible if the community is comfortable with the potential abandonment or unenforceability of certain intellectual property rights.

When an initial development team retains control over trademarks or copyrights associated with the protocol, crypto-asset holders may reasonably expect a profit from that team's offensive use of the trademarks or copyrights. The same expectation of profit is inherent in any decentralized structure that contributes, in a coordinated manner, to off-chain activities, except for when all other off-chain activity is distributed across other decentralized entities.

To mitigate this risk, development teams or overly coordinated communities should consider issuing a public statement, or publishing extremely permissive brand guidelines evidencing that they will use their intellectual property rights only for defensive purposes and not for offensive purposes. It is important to abide by those statements and guidelines after they are made and published.

Governance Decisions

Decentralized governance systems are designed to empower any crypto-asset holder to make a proposal, vote on the proposal and delegate voting rights to those with greater knowledge or interest in the proposal. Crucially, these proposals are self-executing: they allow anyone to make and vote for proposals, which are then automatically implemented if successful.

Implementations vary around the number of crypto-assets required to make a proposal, the number of votes required for a proposal to pass and the number of affirmative votes.⁹ In some

⁹ See, for example, Compound's governance system, [described here](#).

governance systems, crypto-asset holders stake crypto-assets to increase their voting power. The increase is often based on the length of the staking period to empower those who have the greatest economic interest in the protocol.¹⁰

Effective governance systems prioritize simplicity and attempt to encourage a broad range of participants to engage in governance. However, web3 development teams have focused on improving protocols, which they view as a crucial, high impact activity, rather than improving governance systems, which they consider less important. Consequently, the development of decentralized governance systems has remained largely stagnant.

To further decentralize, governance systems must develop appropriate crypto-asset ownership thresholds for quorums, proposals and voting; simplify mechanics for proposals; create benefits for participation in governance; eliminate multi-signature wallets that hold broad authority over protocols; and improve tools for communications and crypto-asset payments. Developers should create code for basic, repeatable proposals, such as changing a common parameter, to increase the participation among the less sophisticated crypto-asset holders. Communities should consider seeking assistance from third parties who can provide [insight to the community](#) on complex topics that the community would struggle to evaluate on its own.

Initial development teams should also consider issuing a public statement that they will not participate in governance to ensure holders of crypto-assets cannot expect profits in reliance on the teams' governance efforts. Teams that do so must abide by their statement.

Community and Legal Structuring for Efficient Off-chain Activities

A community's structure plays a meaningful role in its ability to decentralize off-chain activities and maintain operational efficiency while failing the *Howey* test. Structure should be considered from three perspectives: (1) how individuals and groups within a community organize themselves, (2) how intra-community structures communicate, and (3) the legal structures used to engage in off-chain activities.

How can communications be approached to effectively decentralize off-chain activities?

After identifying the off-chain activities that can be decentralized and outlining what decentralization looks like, one question remains: How should community members interact with each other to implement that decentralization?

¹⁰ See, for example, Curve's governance system, [described in Chapter 8 of the Curve Documentation](#).

Community Structures

Core to any implementation is how a community structures off-chain activities. Web3 communities structure themselves in four main ways:

1. All community members can take part in each decision.
2. The community is split into informal, undefined groups that receive funding from the community, known as subDAOs. These groups operate independently without any meaningful direction from the community as a whole.
3. The community is split into formal, community-defined subDAOs that address specific off-chain activities. These subDAOs operate independently but receive directions from the wider community.
4. The community provides direction to a legal entity, typically a foundation or trust, that carries out all activity on behalf of the community.

SUFFICIENT DECENTRALIZATION:
A PLAYBOOK FOR WEB3 BUILDERS AND LAWYERS
BY MARC BOIRON

How are web3 communities typically structured?

Web3 communities tend to structure themselves in one of four ways:

1. All community members take part in every decision
2. Community is split into informal, undefined groups - subDAOs that operate independently.
3. Community is split into formal, community-defined subDAOs that receive clear direction.
4. Community provides direction to a legal entity - often a trust or foundation - that carries out activity on behalf of the community



In the past few years, communities have made use of subDAOs, both formal and informal. Each community determines the level of coordination among subDAOs. For the purposes of securities law compliance, subDAOs can fall on extreme ends of a spectrum. They are either:

- so efficiently coordinated that they would, collectively, be considered an “active participant” – the “others” in the “efforts of others” prong of the *Howey* test; or
- so inefficient and uncoordinated that their members do not know anything the public could not easily find out. An investor could not reasonably rely on any such subDAO to

produce profits. These subDAOs could not be collectively viewed as an “active participant,” so the *Howey* test would fail.

Every community’s goal should be to decrease the coordination of the first group and increase the efficiency of the second group, in each case in a manner that fails the *Howey* test.

The “ideal” community would further split subDAOs into “supported subDAOs” and “operations subDAOs.”

Supported subDAOs handle all off-chain activities that create value in the protocol, which can also drive value in the related crypto-asset. These generally will include the following:

- protocol development;
- business development;
- growth and marketing;
- intellectual property; and
- governance decisions.

Operations subDAOs are subDAOs that provide support to supported subDAOs. These generally include:

- Finance – Aggregates on-chain data about the protocol’s financial performance ([as Yearn has done historically](#)), submits budget recommendations for subDAOs to the broader community, and holds funds used to pay subDAO contributors.
- Legal – Publishes legal analysis about the protocol and provides legal advice to subDAOs.¹¹
- Recruiting and personnel – Recruits candidates for subDAOs and other operations, either as full-time employees or independent contractors.
- Administration – Handles contracts with third parties that provide subDAOs with tools, such as software, payroll providers, and payments. Manages all other administrative matters for subDAOs.

Operations subDAOs should empower supported subDAOs to be as independent from one another as possible. For instance, the legal subDAO should always publish guidance in the public domain and create accessible legal forms for other subDAOs to use. The legal subDAO could also help other, similarly structured communities by making these forms easy to use. The finance subDAO could publish financial models specific to web3 and teach the wider web3 community how to build a budget and manage runway across subDAOs. The recruiting subDAO could provide public guidance on hiring and compensating quality candidates.

¹¹ Creating a legal subDAO may be difficult because few legal counsel are willing to provide advice through a DAO. A law firm can provide these services to ensure that discussions remain attorney-client privileged. That said, [analysis](#) similar to the one published by Gabriel Shapiro is what legal subDAOs can do for the benefit of the community and will be beneficial to all but no longer privileged.

The number of supported subDAOs is a tradeoff between the efficiency of centralization and the reduced legal risk of decentralization. The most efficient (but least centralized) structure would incorporate all off-chain activities into one subDAO. The least efficient (and most decentralized) structure would split each activity into a separate subDAO. When the community has decided on the appropriate number and functions of subDAOs for its purposes, it should create subDAOs for each activity and form an appropriate entity.

As a practical matter, all communities require an administrative subDAO, whether it stands alone or is combined with other operations subDAOs. Otherwise, nothing will get done operationally. A community also requires an administrative subDAO (and the advice of a legal subDAO) to form supported subDAOs. Once created, the recruiting subDAO should hire community members to join the supported subDAOs. Hiring employees, rather than independent contractors will add administrative and tax complexities. However, it may be necessary if the subDAO member acts like an employee.

When funding subDAOs, the funds necessary to organize and form each subDAO can be transferred from a grants program that has broad enough approval from the community or be directly transferred from a community treasury. To maintain independence from other subDAOs, independent proposals to fund and form each subDAO are preferable.

Effective Communications

As contractors and employees are recruited to join the subDAO, the administrative or operations subDAO should put in place a means of communications, whether it be Discord, Keybase or another tool, for all of the subDAOs engaging in off-chain activities.

Without proper structure and communication tools, communities are likely to begin to operate like one company, at least as far as the *Howey* test is concerned. They may become like a typical company, where business units sit nearby other business units and closely discuss issues. That is to say, companies are private – nobody outside of the company knows what is going on, and cannot contribute to whatever happens inside the company. Only the employees can create value.

Web3 communities must not become similar to companies in this manner. Coordination must be minimized by making communications public. Each subDAO must communicate in a public domain so members of each subDAO can access the information contained within their messages.

Public communications should be comprehensive, including (1) daily discussions among members of the subDAO on public channels, such as Discord, or other communications platforms; (2) timely, detailed updates on completed projects posted in writing or video on

Notion or similar publicly-accessible products;¹² and (3) roadmaps of future projects and the status of those projects, posting them on Notion or similar products.¹³

When communications are public, subDAOs can operate with full context around the decisions they make. In addition, since everything is public, no subDAO holds onto private information that could create value for the crypto-asset. No group within the community, or even the community as a whole, holds information that others do not also hold.

This communication structure also means that community members who are not part of subDAOs can make valuable contributions to the community. Indeed, community members should not have to be part of a subDAO at all; they should have the tools to contribute regardless.

While engaging in these activities, subDAOs may acquire information that is meaningful to the value of a crypto-asset and fail to make it public. However, decentralizing subDAOs should mitigate the risk that this information would harm holders of crypto-assets that are not members of a subDAO.

In particular, each subDAO will lack information held by other subDAOs, such that no member of a subDAO that holds meaningful information could use that information to the detriment of crypto-asset holders. Even if subDAOs collectively held enough material non-public information that they would have to disclose their collective information under U.S. securities laws, they should not be sufficiently coordinated to all work together to make the disclosures that are, collectively, material.

Consequently, an investor could not look to any subDAO, or even to a collective of subDAOs, and reasonably expect a profit from their efforts. Only the individual efforts of each subDAO, based on public information, create value in the crypto-assets.

Alignment on Mission, Vision and Values

Communities should consider creating alignment on a common mission, vision, and set of values. These can assist with decentralization by reducing the amount of close coordination necessary among contributors who understand guiding principles and goals. They empower individual contributors to act independently and provide a guidepost when contributors are presented with ambiguous situations. Admittedly, the creation of mission, vision and values can create centralization when they are created in a centralized manner and the person or team creating them reject changes the community suggests and considers them anyway to be community-adopted mission, vision and values. It is critical that they truly align with the community broadly and may need to change once in a while as the community changes.

¹² For an example on the product side, see <https://linear.app/changelog>.

¹³ Although this playbook uses examples of web2 tools, a number of similar web3 tools are in development, such as [Comm](#), an alternative to Discord, and [Anytype](#), an alternative to Notion.

What legal entities should subDAOs use for off-chain activities?

Legal entities, such as foundations and trusts, can protect the community or benefit specific community members. They do not directly contribute to decentralization but can lead to centralization.

The optimal structure for decentralization would construct a separate legal entity for each community member. This would protect each member that contributes to the community but would be expensive and impractical. The most centralized structure would funnel all of the community's off-chain activities through a single legal entity. This would be efficient but the centralization could cause problems with securities law compliance.

A practical middle ground would create between five and ten entities to carry out different, and at times overlapping, off-chain activities. These entities should map out to each subDAO to protect community members that contribute to that subDAO. This would limit their liability, provide the authority to sign contracts and ensure that a subDAO complies with taxes.

It is not necessary to use the same legal entities for all subDAOs. A foundation may be appropriate for one subDAO, a trust for another and an unincorporated nonprofit association (UNA) for a third.¹⁴

The entity a community chooses for a subDAO depends on its goals, the location of community members and the demands for decentralization. SubDAOs should consider the use of (1) a foundation created in the Cayman Islands or British Virgin Islands,¹⁵ (2) a trust created in

¹⁴ Several articles have been written on potential entity types that communities may choose to use. See a16z's "[Legal Framework for Decentralized Autonomous Organizations](#)" for a comprehensive analysis of entities used in web3 communities (with a detailed consideration of trusts); "[Legal Wrappers and DAOs](#)" for a comprehensive analysis of all entities used in web3 communities (without a detailed consideration of taxes); and dYdX Foundation's "[Legal Framework for Non-U.S. Trusts in Decentralized Autonomous Organizations](#)" for a comprehensive analysis of Guernsey trusts used in web3 communities, including tax considerations, without a discussion of other entity types.

¹⁵ As a side note, a common practice has arisen where an initial development team forms a foundation that requires directors of the foundation to take direction from crypto-asset holders. This practice may not achieve the team's intended purpose. Web3 builders and lawyers believe that approach helps decentralization; instead, it creates a reliance on the foundation – the issuer of the crypto-asset – to engage in off-chain activities that may increase the value of related crypto-assets. In most cases, the foundation will have a services agreement with an entity created by an initial development team and request services under it. Depending on the nature of the crypto-asset holders' requests to the foundation, the crypto-asset holders may actually be indirectly requesting services from the initial development team, weakening the team's position that the crypto-asset holders do not rely on its efforts to create value in a crypto-asset. Instead, web3 builders and lawyers should consider creating a foundation that does not receive direction from the community but has a purpose that is entirely aligned with the community, resulting in the foundation seeking voluntarily to assist the community in developing robust off-chain activities. The community can then create subDAOs as contemplated in this playbook. This approach creates greater distance between the initial development team and the community in a manner that decreases the crypto-asset holders' potential expectation of profit from that team's efforts. If the foundation is active and independent from the crypto-asset holders and the initial development team, then it also can add to the decentralization of off-chain activities that create value in a crypto-asset.

Guernsey or Jersey, and (3) an UNA existing under U.S. state law.¹⁶ In certain circumstances, other entity types or jurisdictions may be more appropriate choices.

In brief, the following chart lays out the advantages and disadvantages of each entity type, or not using a legal entity at all.

Comparing Legal Entities for subDAOs

The entity that a community chooses for their subDAO depends on its goals, the location of community members and the demands of decentralization.

	NO ENTITY	CAYMAN FOUNDATION	GUERNSEY TRUST	US-BASED UNA
Government Filing	No	Yes	No	Maybe*
Tax Liability	Maybe	No	No	Yes
Limited Liability	No	Directors	Trustees	Members
Legal Person	No	Yes	No	Yes
Contract Signing	No	Yes	Yes	Yes
Censorship-Resistant	Yes	No	Yes	Yes
Hire Contractors and Employees	No	Yes	Yes	Yes
Operational Difficulty	High	Low	High	Moderate
Revenue Distribution	Yes	No	Maybe	Sometimes

* Required only in a limited number of states.



Impact of Cross-Community Support on Decentralization of Off-Chain Activities

The most effective way for a community to decentralize its off-chain activities is with the help of other communities. Web3 communities that openly share tooling and best practices on procedure and communication strategies benefit the whole web3 ecosystem. If each community shared the output of its off-chain activities – or, frankly any of this output – with other communities, off-chain activities would decentralize at a much faster pace as each community would not have to reinvent the wheel.

¹⁶ Other entity types have also been considered but are not viewed as being as viable as those discussed in this playbook including: limited liability companies, cooperatives and for-profit unincorporated associations.

There are several areas where helping other protocols' off-chain activities is sensible: (1) tooling for governance, such as Compound Labs' [governance system](#), which could be used in any community, and Uniswap Labs' [introduction](#) of [Sybil](#), a governance tool for discovering delegates by mapping on-chain addresses to digital identities; (2) legal documentation and forms, such as [dYdX Foundation](#)'s use of trust structures in DAOs and its [Declaration of Trust](#); (3) identifying (i.e., promoting) complementary protocols or applications; and (4) creating best practices in off-chain activities.

Such contributions would not be an act of altruism. If a community provides value to another, the likelihood that other communities return the favor increases. When one community helps out another, then publishes that help in the public domain, unrelated communities can also benefit and may be encouraged to provide additional support themselves. With time, the resources available to communities will provide significant value to those who contribute.¹⁷

Venture capitalists can also play an important role given the breadth of their portfolios. If a common problem arises in their communities, venture capitalists can address the problem at once for all communities – no matter how active they are in a specific community. If a common solution is widely adopted, a specific community would have even less access to material information.

The efforts that other communities and venture capital firms put into a community can meaningfully impact a *Howey* analysis. At scale, those efforts can create significant value in crypto-assets that lead their holders to rely less on the initial development team or another active participant to produce value in the crypto-assets.

If just a handful of high-impact communities and venture capitalists provided cross-community support, then reliance on the efforts of the initial development team or any other active participant could be diminished. This would reduce the risk of centralization, and thus the regulatory risk, and increase the speed of all communities engaged in off-chain activities.

Role of Initial Development Team in Off-Chain Activities

Initial development teams that engage in off-chain activities increase the risk that the community reasonably expects profits in reliance on their efforts. This leads those teams to back off from playing too significant of a role in off-chain activities.

When communities take over significant off-chain activities, as outlined in this playbook, initial development teams have more room to engage in off-chain activities as communities are less likely to reasonably expect profits by relying on those teams' efforts.

Put another way, the initial development team is less important when the communities engage in those activities. Communities then benefit from the fact that the initial development team

¹⁷ As always, certain communities will freeride on the efforts of others. That exists across all open-source efforts (and any other efforts that provide a public benefit) and is difficult to avoid.

can remain more meaningfully involved in growing the protocol, even if their contributions are outsized by community efforts.

Initial development teams should pay attention to more than just their off-chain activities. They should also avoid:

- Creating an expectation that crypto-assets transferred to the initial development team incentivizes them to increase the value of those crypto-assets. Although that often will appear to be the case, it is not a given that a team holding crypto-assets will seek to create that value.
- Promoting the success of the initial development team's efforts. Most teams will want to publish their successes, but they should seek to counter-balance those publications by promoting community achievements in which they were not involved. Ideally, that team does not need to counter-balance publications because the community has contributors focused on communications regarding the community's activities, including those of the subDAOs.
- Making statements regarding centralization that implies a reliance on a centralized party's efforts. A balance should be struck between openly disclosing the risks of a protocol and disclosures that result in potential liability.
- Discussing off-chain activity or the on-chain operations of the protocol in a way that implies the initial development team performs certain actions. English teachers will always teach students to write in the active voice but all descriptions of off-chain and on-chain activity should be in the passive voice. The passive voice accurately describes on-chain activity and avoids creating any expectation of profits in any groups' off-chain activities.
- Posting or sharing social media content without an expectation that the initial content will be attributed to the team sharing it. If teams do not agree with the content of tweets they retweet, then they should make that clear.
- Referring to initial development teams in terms that imply an increased importance relative to others, such as "lead" or "core" teams. Instead, they can be referred to as "initial contributors."
- Participating in the governance of the protocol. When the initial development team participates in governance, crypto-asset holders continue to rely on that team to create value by making strategic decisions that are included in proposals, rather than allowing the community to make those decisions.

Initial development teams could argue that some of the actions above would not cause a third party to reasonably expect to profit from their entrepreneurial or managerial efforts. For example, private discussions with an exchange to list a crypto-asset for trading, which are unknown to the public, should be considered to create an expectation of profit from any team's efforts because the team's efforts are unknown to the public. However, perception matters; it is preferable to avoid needing to address the issue.

Although this playbook is intended to address only “sufficient decentralization,” initial development teams should consider actions that could prevent them from taking the position that crypto-asset holders do not have a reasonable expectation of profit, including:

- Taking any action to list crypto-assets on a secondary market, whether a centralized or decentralized exchange; acting with another party, such as a market maker, to do the same, or promoting the existence of a secondary market that another party may create.
- Making any statement about the price appreciation of the crypto-assets, or creating an expectation of profit that does not yet exist.
- Discussing the market structure around the crypto-asset, such as liquidity, selling pressure and demand.

Conclusion

There is no perfect way to achieve sufficient decentralization. In the months and years ahead, communities in web3 will test innumerable ways of pursuing sufficient decentralization across all of the off-chain activities outlined above. More web3 native tools for communities will be created and evolve in ways that will facilitate communications between teams and structures they use to operate effectively. As long as communities maintain the principles of openness in this playbook, sufficient decentralization while engaging efficiently in off-chain activities will be achievable.

The analysis expressed in this playbook is the author’s own analysis written in his personal capacity and not on behalf of Variant (Unofficial Management, Inc.) or its affiliates (“Variant”). Although the author is a strategic advisor to Variant, the views expressed in this playbook do not necessarily reflect the views of Variant.

This playbook is provided for informational purposes only, and should not be relied upon as legal, business, investment, or tax advice. Thus, this playbook should not be construed as legal advice for any particular facts or circumstances and is not meant to replace competent counsel. It is strongly advised for you to contact reputable legal counsel in your jurisdiction for any questions or concerns. None of the opinions or positions provided in this playbook are intended to be treated as legal advice or to create an attorney-client relationship. This analysis might not reflect all current updates to applicable laws or interpretive guidance, and the author disclaims any obligation to update this playbook.

References to any securities or digital assets are for illustrative purposes only, and do not constitute an investment recommendation or offer to provide investment advisory services. Furthermore, this playbook is not directed at nor intended for use by any investors or prospective investors, and may not under any circumstances be relied upon when making a decision to invest in any fund managed by Variant. Any investments or portfolio companies mentioned, referred to, or described are not representative of all investments in vehicles managed by Variant, and there can be no assurance that the investments will be profitable or that other investments made in the future will have similar characteristics or results. A list of investments made by funds managed by Variant (excluding investments for which the issuer has not provided permission for Variant to disclose publicly as well as unannounced investments in publicly traded digital assets) is available at <https://variant.fund/portfolio/>. Certain information contained in this playbook has been obtained from third-party sources, which may include portfolio companies of funds managed by Variant. Variant has not independently verified such information and makes no representations about the enduring accuracy of the information or its appropriateness for a given situation.