

Professional Perspective

Legal Implications of Decentralized Autonomous Organizations

Mark Cianci, Evan Gourvitz & Kelley Chandler,
Ropes & Gray & Raffi Teperdjian, Protocol Labs

**Bloomberg
Law**

[Read Professional Perspectives](#) | [Become a Contributor](#)

Reproduced with permission. Published April 2022. Copyright © 2022 The Bureau of National Affairs, Inc.
800.372.1033. For further use, please contact permissions@bloombergindustry.com

Legal Implications of Decentralized Autonomous Organizations

Contributed by *Mark Cianci, Evan Gourvitz & Kelley Chandler,*
Ropes & Gray & Raffi Teperdjian, Protocol Labs

Businesses built around emerging technologies are evolving at a rapid pace. Although predicting the direction of advances can be tricky, it seems clear that decentralized autonomous organizations (DAOs)—quasi-corporate management structures organized through blockchain—will be important to the next wave of development.

Over the past few years, DAOs have been gaining attention in the decentralized finance (DeFi) world both as a new form of governance and as the subject of various enforcement actions. These trends, in turn, raise a number of strategic and regulatory considerations for those working with, or contemplating the adoption of, a DAO management structure. This article explores what DAOs are and how they function, how DAOs can be created and structured, and several key legal considerations associated with DAOs.

Terminology and Background

To understand DAOs, it first is necessary to understand “blockchains” and “smart contracts.”

Blockchains are fundamentally decentralized databases enabled by defined protocols (rules for formatting and processing information) expressed in computer code. Each blockchain varies in terms of the sophistication of the protocol, the ways in which users interact with the protocol, and the protocol's governance. These variations allow blockchains to perform different functions.

Basic blockchain protocols can be designed to perform simple functions, such as exchanging value—e.g., the Bitcoin blockchain—or representing ownership of digital or physical assets—e.g., non-fungible token (NFT) blockchains. More sophisticated blockchain protocols can enable automated or “smart” contracts that can perform complex financial and other transactions without the need for third-party intermediaries. DAOs are essentially advanced smart contracts that use programmable blockchain protocols to automate transactions and corporate governance through tokens. Smart contracts enshrine the rules of the DAO in code and hold its treasury.

When a DAO is created, its developers usually retain initial control over its protocols to oversee development as it gains membership. An individual or entity gains membership in a DAO by purchasing DAO tokens. These purchases generally occur either through direct peer-to-peer digital wallet transactions or via decentralized “swapping” platforms, whereby digital wallets holding widely used cryptocurrencies—e.g., Ethereum or Binance Coin—can exchange these assets for DAO tokens.

The DAO tokens, in turn, give purchasers the ability to participate in the DAO community according to the rules of the DAO's protocol—e.g., voting on organizational membership requirements, making governance decisions, choosing how the DAO invests its treasury, etc. Along with growing the membership of the DAO, the sale of DAO tokens also funds the DAO's treasury.

Once the community and functionality of the DAO are sufficiently developed, developers typically pass control of the smart contracts to its members—i.e., the holders of the DAO's governance tokens—by fully deploying and releasing the DAO on a smart contract-capable blockchain. At that point, the DAO's developers no longer are able to influence the organization's decisions any more than the DAO's other tokenholders, and all decisions regarding the DAO are made collectively by the tokenholders according to the rules encoded in the DAO's governance smart contracts.

Legal Implications

Unsurprisingly, DAOs raise a variety of legal issues, including in relation to corporate formation and governance, contracting, securities regulations, intellectual property law, and data privacy and cybersecurity requirements.

Formation & Contract Law

For individuals and businesses planning to use the DAO model, formation has presented certain challenges. While a handful of U.S. jurisdictions, such as Wyoming and Vermont, and non-U.S. jurisdictions including the Marshall Islands, have provided a clear pathway for DAOs to be integrated into traditional legal structures, DAOs currently are not recognized legal entities in most jurisdictions. The mere act of encoding and making a DAO available to the public does not necessarily create a legal entity, and developers interested in giving their DAO a legal framework generally must deploy bespoke solutions to do so. Currently, two DAO structures are gaining traction: the “unwrapped” DAO and the “wrapped” DAO.

An unwrapped DAO is a form of organization generally unrecognized by current U.S. law, and thus is unprotected by the limited liability afforded to limited liability corporations (LLCs), limited liability partnerships, and other corporate legal entities. Absent a legal form, courts might find that the DAO's members had formed a general partnership as a matter of law, with each individual DAO member (i.e., each DAO tokenholder) taking on personal liability for the activities of the entire DAO.

This may be a significant concern for participants, since many individual tokenholders may not intend to expose themselves to the various legal and compliance risks that could arise in connection with a DAO.

Moreover, if a DAO with no associated legal entity is found to be a general partnership, any individual DAO member theoretically could enter into contracts and bind the other DAO members without their knowledge or consent. Additionally, although DAO members could authorize a single member to enter commercial contracts on behalf of the whole organization, both the authorized member and the other DAO members still might face unlimited personal liability for any claims arising from such agreement unless the passive DAO members individually contracted with the counterparty to impose limitations to their individual liability.

Absent further legislative or regulatory action, the rights, obligations, and potential liabilities for unwrapped DAOs' tokenholders and contracting counterparties are highly uncertain in most jurisdictions.

Wrapped DAOs, however, provide additional certainty although are by no means a perfect solution. In a wrapped DAO, all or a subset of the DAO's members create a formal business organization—often a corporation or LLC—that manages and/or owns certain aspects or functions of the DAO's ecosystem, such as the DAO's smart contracts and its treasury. Associating a DAO with such an entity may—depending on the precise structure deployed—provide a platform for achieving limited liability and may enhance the DAO's ability to contract and exchange services and payments with third parties, as well as to engage in commerce more generally.

To be most effective, the LLC or other corporate organization developed for the DAO should have a sufficient nexus to the broader DAO community and ecosystem in order to assure tokenholders and counterparties that the DAO as a whole falls under the corporate form. Given the nascent emergence of DAOs generally, and wrapped DAOs in particular, the degree to which a DAO's association with an LLC or other business organization will provide the broader DAO ecosystem with limited liability, and the ability to contract with traditional counterparties, remains untested.

Securities Laws

To ensure compliance with U.S. securities laws, when a DAO issues tokens that are not registered with the Securities and Exchange Commission, its organizers should either satisfy themselves that such tokens are not securities or ensure that the tokens are issued pursuant to an exemption from registration.

Under the Securities Act of 1933, every offer or sale of a security must either be registered or subject to an exemption from registration. Section 2(a)(1) of the Securities Act defines securities to include “investment contracts.” In *SEC v. W.J. Howey Co.*, the U.S. Supreme Court established the framework for analyzing whether an asset is an investment contract subject to the securities laws. Under *Howey*, an investment contract is a contract, transaction, or arrangement whereby a person invests money in a common enterprise and expects to receive profits on that investment resulting from the efforts of the enterprise's promoters or others.

The SEC first prominently asserted that the *Howey* analysis applies to cryptocurrencies in its July 2017 [Report of Investigation into DAO Tokens](#). After “The DAO”—the name of a specific DAO created by a German startup in 2016—was hacked and litigation ensued, the SEC found that tokenholders' contributions of Ethereum in exchange for tokens of The DAO constituted an “investment of money,” and that the efforts of The DAO's founders and curators were essential to the

functioning of The DAO. The DAO's founders and curators also pooled the contributed Ethereum to fund projects from which The DAO's tokenholders eventually stood to profit. These facts led the SEC to conclude that The DAO's tokens fell squarely within the purview of *Howey*, constituting a security.

The SEC's subsequent *Munchee* cease-and-desist order in December 2017 promulgated additional factors to be considered when determining whether a DAO or other cryptocurrency token is a security, including the immediate usability of the tokens, the presence of the tokens on the secondary markets, how the tokens are advertised, and how the proceeds from an offering will be used. Despite the enumeration of numerous factors, which might suggest a somewhat flexible approach to the characterization of tokens as securities, the SEC to date has never indicated that any tokens or cryptocurrencies—other than Bitcoin and Ethereum—are not securities. In fact, the SEC's recent enforcement activity and ongoing litigation positions indicate that the SEC's interest in challenging unregistered securities offerings in the crypto space is only intensifying.

For example, in February 2022, the SEC joined several state enforcement agencies that charged BlockFi Lending LLC in 2021 with failing to register its crypto lending product as a security. BlockFi had advertised its ability to generate returns for investors who loaned digital assets to BlockFi. These assets were then pooled, loaned, and invested at BlockFi's discretion, with the goal of generating profits. The SEC found that BlockFi's investment product met the factors of the *Howey* test and that BlockFi's offering of this product to retail investors did not qualify for an exemption from registration.

To resolve the enforcement action, BlockFi was required to pay \$100 million in penalties—one of the largest penalties to date in the digital assets space. Similarly, in an ongoing lawsuit initiated in late 2020 against Ripple Labs Inc., the SEC is alleging that the company's offering of its cryptocurrency asset, XRP, meets the *Howey* test and constitutes an unregistered securities offering.

Additionally, DAOs will increasingly need to consider the regulatory landscape with respect to any NFT assets. Particularly in the case of fractionalized NFTs, where the ownership of physical or digital assets is divided into many units and sold to diffuse investors through tokenization, the SEC has indicated that such tokens may be securities under the *Howey* test.

No DAO has successfully registered its token offering to date, and where DAOs attempt to register their token offerings as securities, it is important to recognize that registration statement disclosures must be sufficient and complete. For example, in late 2021, the DAO American CryptoFed DAO LLC, which was organized under Wyoming's recently enacted statute recognizing DAOs as a unique corporate form, attempted to register two digital tokens.

The SEC brought an action against CryptoFed, alleging that the DAO did not include sufficient information about its tokens in its registration statement. The CryptoFed example serves as a reminder that DAOs and others in the cryptocurrency space that do register their tokens with the SEC must ensure that their disclosures contain no material misstatements or omissions and fully disclose the risks associated with investing in the tokens.

As digital assets become more popular, and both the courts and the SEC are increasingly required to grapple with what constitutes a security, DAOs eventually will be able to make more informed decisions regarding whether to treat their tokens as securities. In the meantime, DAOs that choose neither to register their tokens as securities nor to avail themselves of a registration exemption could face enforcement and private litigation risk stemming from the possibility that their tokens ultimately may be characterized as securities.

Licensing, Copyrights & Software Code

DAO participants unquestionably will be faced with how to ensure ownership and enforcement of the intellectual property they generate and acquire as they continue to grow and develop. Ownership and licensing of the IP associated with DAOs, such as copyrights and software code, are becoming increasingly important. In the case of software, if a DAO's underlying software is sufficiently creative to constitute an "original work of authorship," then it likely is protectable as a matter of law—as long as a discernable entity authored and owns the software and can assert it against another discernable entity or individual.

If the DAO is wrapped and implements traditional IP ownership assignments from the author(s) to the associated entity in place, then copyright ownership may be a straightforward question. If a DAO is unwrapped, however (or if there are no IP assignments from DAO members who authored the protocol to the associated entity), there is an open question about

exactly who owns that underlying software, especially depending on how many members the DAO has and who contributed to the development and improvements upon that software.

Moreover, in the licensing context (especially for unwrapped DAOs), it may be unclear who or what actually is the licensor or licensee where a DAO seeks to license either valuable software code or copyrights related to other DAO assets, such as NFTs.

Recently, Curve DAO fielded a proposal that it should hire counsel in the U.S. and other relevant jurisdictions to prevent other DAOs from “wholesale copying” of its code. Subsequently, a poll on Curve's forum revealed that sixty-seven percent of the membership agreed. The proposal came after Saddle DAO, a less prominent DAO allegedly copied Curve DAO's code, claimed ownership of the copyright therein, and granted a license to that code to anyone in the world.

Curve DAO's dilemma represented a significant development, especially because there has been pushback in the DeFi world against DAOs or other entities attempting to enforce their IP rights, which is seen as contrary to the radically open-source culture and ethos of DeFi. Critics of extensive IP licensing in the DeFi space worry that it may stifle innovation and discourage talented programmers from joining DAOs. As with Curve DAO, however, DAOs may start to take protecting their valuable IP more seriously.

Trademark Law

As is the case with contracting and licensing, a DAO's ability to both own and enforce a trademark may depend on its organizational structure and legal status. For wrapped DAOs, it will be easier to identify the entity that uses the trademark associated with the organization in commerce, and to assert an action for enforcement of that trademark. For unwrapped DAOs, however, trademark issues will likely be more complex due to the inherent difficulties in determining ownership, use in commerce, and the right to enforce the mark.

It will be interesting to see how trademark issues pan out in the context of unwrapped DAOs, especially because [federal case law](#) from the Ninth Circuit and a few other circuits has held that unincorporated associations have the capacity to own trademarks. It is possible that an unwrapped DAO could attempt to enforce its trademark under a similar theory and be successful in federal court, although it could have difficulty proving that its mark serves as an indicator of source.

IP Infringement

Another challenge with respect to IP enforcement is determining the proper defendant(s) when the infringing entity is an unwrapped DAO. Even if the plaintiff has all of the appropriate legal structures in place to enforce its IP—i.e., legal entity, IP assignments, registrations, etc.—if an unwrapped DAO is the infringer, it may be unclear what party or parties properly should be named.

If its members are easily identifiable, holding them collectively liable as a general partnership may be feasible. If not, it's possible that the plaintiff could locate one or more DAO members, name them as parties to a lawsuit, and proceed under a theory of joint and several liability. This would leave the named parties to pursue relief and judgment against the other members of the DAO. Such an approach would be less than ideal, however, because the prevalence of anonymity in the DeFi and DAO world might make it difficult or potentially impossible to find all of the relevant people or entities, preventing the aggrieved party from obtaining full relief for infringement.

Data Privacy Law

As legislation on consumer data privacy and cybersecurity continues to grow and become more robust, lawmakers have placed the onus on companies to provide careful oversight when collecting, storing, and using data that can be linked to individuals' identities. Legislation such as the California Consumer Privacy Act, Europe's General Data Privacy Regulation (GDPR), and a growing number of other laws contain broad notions of consumer protection and indicate that personal data includes any consumer data that can be linked to an individual.

Most notably, under the GDPR, individual consumers are considered “data subjects” with corresponding rights such as the right to be informed, to access data collected about them, to rectify incorrect data, to erase data, etc. Such rules apply to the “data controllers” who own the responsibility for the data and “data processors” that handle consumer data on behalf of data controllers.

In a DAO, however, members generally are assumed to have partial ownership in the organization and to have a say in its governance. This means that members can contribute to the underlying protocol, which makes it difficult to categorize

who owns or controls the data for purposes of privacy. Further, due to the public, permissionless, and practically immutable nature of many blockchain protocols, there likely would be no option for “erasure” with respect to data collected on a blockchain.

Some EU data protection authorities have expressed blunderbuss concerns about all blockchain technologies, even as other EU regulators have embraced these technologies. Several crucial questions remain unanswered in this area: How will highly decentralized DAOs, and blockchains more generally, comply with data privacy laws? Which data privacy laws are applicable to DAOs? If a DAO is highly decentralized and its members are anonymous, how will the applicable data privacy laws be enforced against it?

Until legislators further address the inherent characteristics of blockchain technology, the path to achieving full compliance with privacy laws may be unclear for DAOs. For now, DAOs will have to contend with striking a balance between collecting and processing consumer data and fully embracing the promises blockchain technology offers.

[Ty Owen, Ropes & Gray](#), contributed to this article.