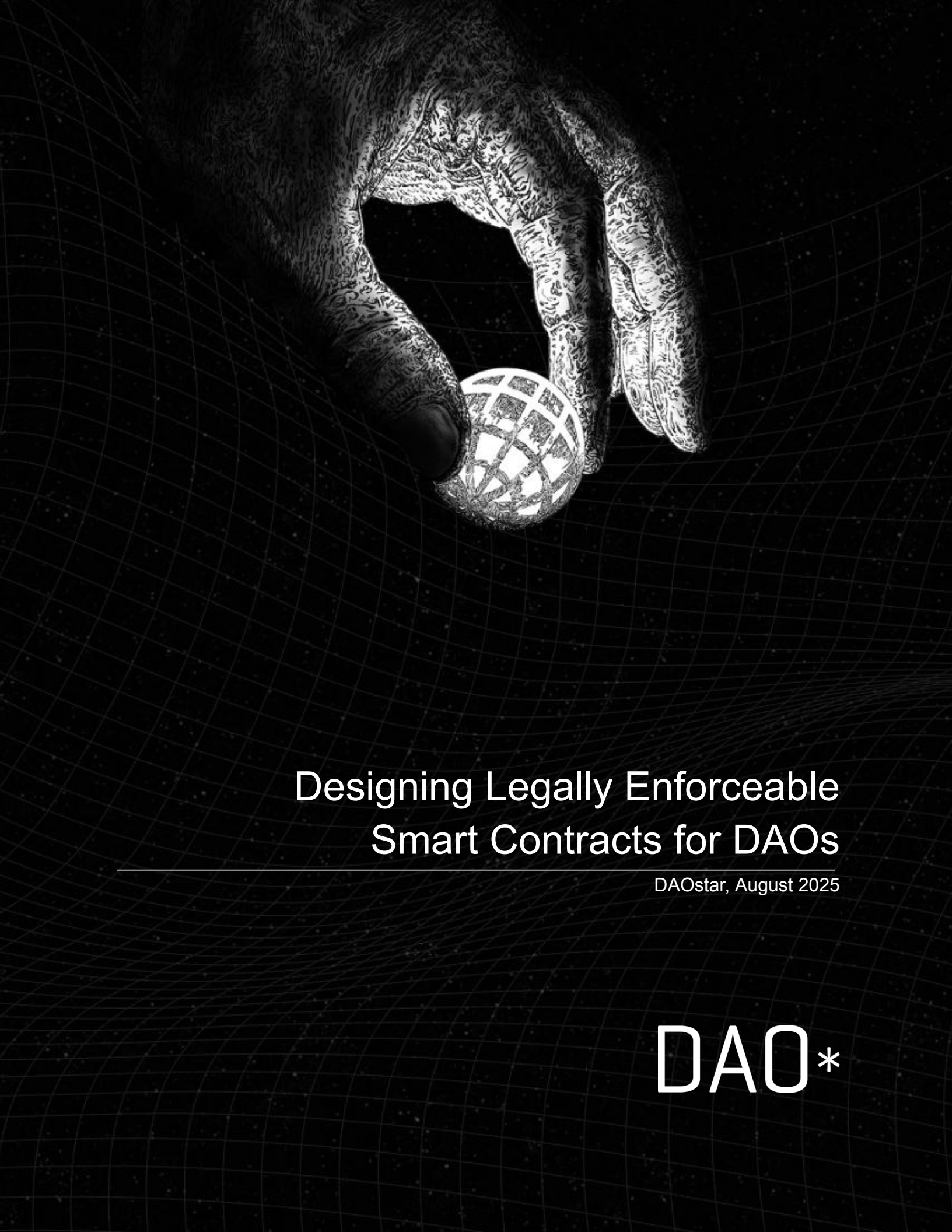

# Designing Legally Enforceable Smart Contracts for DAOs

DAOstar, August 2025

DAO*

# Executive Summary

This paper examines how smart contracts underpinning DAOs can be designed for legal enforceability through the lens of the UNCITRAL Model Law on Automated Contracting, which provides a strong international benchmark with potential for consistent global recognition of smart contract-based systems. It highlights the importance of meeting established contract law principles and focuses on practical implementation, exploring how smart contracts can satisfy essential contract elements with DAO-specific examples for clarity.

A key focus is the challenge of attribution, determining legal responsibility for actions undertaken by automated systems. By integrating legal and technical requirements, the paper guides DAO designers in creating smart contracts that are both effective and legally sound. The work concludes with clear, actionable guidelines that support the design of enforceable smart contracts tailored specifically to DAOs.

# About the authors

Sneha Vijayan is a Research Fellow at DAOstar, whose work explores the legality and design of emerging technologies. She works to bridge law and technology through research, community engagement, and the design of practical tools that aim to make justice more accessible.

.

This report is a publication of DAOstar (or DAO*), the standards body of the DAO ecosystem.

# Contents

# I. Introduction

The title of this paper may seem like an oxymoron, especially to those engaging with DAOs as a move towards autonomy and away from State regulation. Although designed to offer a transparent and largely autonomous alternative to traditional institutions, DAOs remain plagued by flaws that prevent them from achieving their intended potential. This has concern has been raised by many in Web3[1]. This paper argues that some of these flaws can be addressed by designing legally enforceable smart contracts to facilitate DAO transactions.

This paper considers two key flaws which limit the potential of DAOs. Namely, (a) abuse of process and (b) the inability to automate certain actions due to technological limits in digital representation. While some argue these issues are best addressed internally through stronger governance, another approach is to explore how established legal protections, particularly contractual protections, can optimise DAOs. For instance, contract law offers fallback enforcement for obligations involving physical performance that smart contracts cannot automate, increasing accountability and discouraging bad faith. Moreover, legally enforceable smart contracts provide added trust and credibility when DAOs interact with external parties unfamiliar with decentralised or automated systems. Contract law provides such a framework to deter abuse, regulate behaviour, and address breaches requiring off-chain remedies. Importantly, contract law is built on the principle of autonomy, focusing on enforcing the mutual will of parties rather than imposing external controls.

This paper explores how the UNCITRAL Model Law on Automated Contracting (MLAC)[2] offers a promising framework to guide such designs. It begins by examining the nature of traditional legal contracts and smart contracts, and how the legal system evolved to accommodate smart contracts. It then analyses the MLAC, which proposes a global framework bridging conventional contract principles with automated, smart contracts. Building on this, the paper outlines essential elements for designing smart contracts recognised by law in the DAO ecosystem. It further considers the critical component of attribution, to clarify how responsibility can be assigned to actions in automated transactions, and explores mechanisms for legal enforceability

[1] This has been observed in https://thedefiant.io/news/defi/buterin-criticizes-governance-tokens
[2] UNCITRAL Model Law on Automated Contracting (2024), G.A. Res. 79/119, Annex IV, U.N. Doc. A/79/17 (2024), available at https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf.

within DAO environments. The paper concludes with practical guidelines that synthesise these legal and technical insights, to support DAO designers in creating potentially[3] legally binding smart contracts that balance autonomy with legal certainty and protection.

[3] The term “potentially” is used here to reflect the non-binding, guidance-based nature of the Model Law on Automated Contracting, as will be addressed in detail in the paper.

# II. Legal Evolution of Smart Contracts

Legal contracts are private laws created by parties and binding only upon those who choose to enter them. This is a consent-based framework where obligations are voluntarily created and enforced. If parties fail to perform their part of the contract, the legal system may be relied on to remedy the breach and enforce the agreed terms. Contracts have existed for thousands of years, with documented examples dating back to Mesopotamian civilisation[4].

The term smart contract[5] was coined by Nick Szabo[6] in 1994 to describe code-based contracts that automate execution without relying on human performance. Szabo's proposition was that by encoding traditional paper-based contracts, contractual performance could be automated, thereby minimising the need to trust humans for execution. Despite the introduction of smart contracts in the early 90's, a formal, globally accepted legal framework for their recognition had not been considered until recently. The popularity of blockchain resulted in some legislations[7] and reports[8], although limited, which recognised blockchain based smart contracts[9]. However, it was only recently that these developments translated into a global recognition of the need to design smart contracts explicitly within the existing contractual framework to ensure their legal status.

[4] Examples include contract-like inscriptions from Sumer (circa 2100 BCE) and provisions in the *Code of Hammurabi* (circa 1750 BCE), one of the earliest known legal codes, which governed issues like debt, wages, and property, and prescribed remedies for breach.
[5] Following the increased popularity of blockchain, the term smart contract has come to refer to self-executing code deployed and enforced on blockchain.
[6] Nick Szabo, *Smart Contracts*, 1994 at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[7]Such as Ariz. Rev. Stat. Ann. § 44-7061 (2017) available at https://legiscan.com/AZ/text/HB2417/id/1497439, and Tenn. Code Ann. § 47-10-202(c) (2018) available at https://legiscan.com/TN/text/SB1662/id/1802160
[8]In 2019, the UK Law Commission identified the need to extend contractual protections to smart contracts.
[9] The definition of smart contracts evolved over time, to now refer to coded, conditional contracts on blockchain.

# III. Model Law on Automated Contracting

Formal discussions to facilitate a legal framework for recognition of contracts generated and executed using code was first initiated by the United Nations Commission on International Trade Law (UNCITRAL)[10] in 2022. These discussions by UNCITRAL Working Group IV[11] resulted in the adoption of the UNCITRAL Model Law on Automated Contracting (MLAC) in 2024. Its key rationale was to develop guidance for the formal recognition of code-based contracts. Although MLAC does not amount to binding law, it offers a predictive framework for how domestic frameworks will evolve.

According to the MLAC's guide to enactment,[12] automated contracting is the practice of using automated systems in the formation and execution of contracts. The MLAC proposes the extension of the status of a legal contract to those contracts which are formed and executed by automated systems. Smart contracts which facilitate DAO transactions fall within the purview of automated systems, as the definition also covers software components.[13] Therefore, under MLAC, smart contracts are recognised both as an automated system used for contract formation and performance, and as a legal contract in itself. In this paper, while addressing the design and components of smart legal contracts, we also explore the critical role these technical contracts play in facilitating both the formation and the performance of contractual obligations.

Under Article 5, a contract cannot be denied legal effect solely due to it being formed or performed by such a system. However, to be recognised as a legal contract, the smart contract must still contain the essential elements of a traditional contract.

---

[10] UNCITRAL is the core legal body of the United Nations system in the field of international trade law, tasked with harmonising and unifying laws governing international trade.

[11] Working Group IV (Electronic Commerce), established by UNCITRAL in 1997, is specifically responsible for developing legal texts and addressing issues related to electronic transactions, including crucial topics like automated contracting, electronic signatures, and identity management. It has also been responsible for adopting laws like the UNCITRAL Model Law on Electronic Commerce (1996) and the United Nations Convention on the Use of Electronic Communications.

[12] Guide to Enactment of the UNCITRAL Model Law on Automated Contracting (2024), U.N. Doc. A/79/17/Add.2 (2024), available at https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf

[13] Ibid, para. 26.

# IV. Designing for Enforceability

According to traditional principles of contract law, a valid contract requires an offer and acceptance, intention to create legal obligations, consideration, capacity, and legality. Consequently, to attain legal recognition, smart contracts must also contain these elements. Unlike earlier UNCITRAL model laws on electronic commerce, such as the UNCITRAL Model Law on Electronic Commerce (1996), which expressly incorporated the functional equivalence principle by equating electronic 'forms' with paper-based ones, the MLAC concentrates on the function and substance of an automated action itself to ensure its legal effect regardless of its form or the level of human intervention.[14] Therefore, in designing legally enforceable smart contracts, there is no need to create digital replicas of these elements. Rather, emphasis should be placed on whether the substance of each element is objectively demonstrated in its context. Although the MLAC does not explicitly use the term ‘objective demonstration’, this standard is inherently incorporated through established contract law principles. It requires that the essential contract elements be identifiable and demonstrable according to how a reasonable person would interpret the outputs and context of the automated system, rather than relying on any party’s subjective, internal beliefs. Having outlined the foundational principles for the legal recognition of smart contracts, we will now examine how each core contract element may be incorporated within these contracts.

## A. Offer & Acceptance

A valid contract is concluded only when there has been a clear and definite offer or proposal and a corresponding acceptance, which communicates the will of the parties. The absence of human interaction does not invalidate the transaction, provided there is objective evidence of mutual agreement. That is, if a reasonable observer would conclude that offer and acceptance occurred, the requirement is satisfied.

[14] Supra note 13, at.paras 14, 27

Depending on applicable law[15] and the subject matter[16] of the contract, offer and acceptance may be conveyed verbally, in writing, or by conduct. Within DAOs, this can take various forms, such as proposals submitted to the DAO or votes cast by its members. For example:

*A smart contract managing DAO-based insurance might automatically accept a claim and trigger a payout based on pre-set, verifiable criteria without human intervention. For instance, if the conditions encoded in the contract are met, such as verified proof of a covered event confirmed by trusted oracles, the smart contract executes the acceptance by releasing funds to the claimant. Such an automatic action reflects valid acceptance of the offer within the DAO framework, provided the system was intentionally designed to operate this way.*

### Contracts formed by third parties using automated systems

When offer and acceptance are carried out by third parties such as developers or operators, assigning attribution may seem complicated. Acts such as developing or coding a smart contract or operating a platform to facilitate actions related to the legal agreement underlying that smart contract may be facilitated by a third party who is not themselves a party to the underlying legal agreement.

Merely developing a smart contract or providing technical infrastructure does not render one a legal party to the contract. For the purpose of identifying the parties to the legal contract, and consequently those against whom the underlying contract is enforceable, the technical smart contract must be distinguished from the underlying legal agreement it facilitates. For example:

*Alice, a member of Di DAO, submits a funding proposal through a smart contract coded by Bell. Although Bell developed the contract, the proposal, the "offer action" is attributed to Alice, who initiated the transaction using her wallet. Bell's role is limited to enabling the infrastructure. Similarly, when DAO members vote through the smart contract to accept the proposal, their actions, not Bell's, constitute legal acceptance.*

---

**15** Applicable law refers to the specific jurisdiction's legal rules (e.g., state, national) that govern the formation and enforceability of the contract.

[16] Subject matter of the contract refers to the specific goods, services, or performance agreed upon, which may dictate formal requirements (e.g., real estate contracts often require writing).

Legal responsibility and enforceable rights, therefore, attach to those who actively initiate or control contract-related actions, not to the developers or platform operators, highlighting the importance of tracing responsibility for the contract's formation and performance to the actual participants. Additionally, the blockchain's public, immutable ledger supports this attribution by permanently recording each transaction and interaction with the smart contract in a timestamped, transparent, and traceable manner. This ensures that actions can be objectively linked to the natural or legal persons who initiated them, reinforcing accountability and enforceability within the DAO ecosystem.

## B. Intention to Create Legal Obligations

For a contract to be legally binding, parties must intend to create enforceable obligations rather than a mere social or informal arrangement. This intention is generally determined objectively by the parties' conduct, such as fulfilling formalities like registering documents, signing, or clear language expressing binding intent. In the DAO context, identifying this intention is crucial to assessing the legal status of underlying smart contracts. Many DAOs operate under a text-based governance document, often called a DAO constitution, which sets out foundational rules regarding operations, decision-making, and resource allocation. For example, the ENS DAO Constitution governs treasury management and amendment procedures.

In some instances, the manner in which a DAO Constitution or related documents are framed, may indicate parties' intention to be legally bound. As several participants join DAOs primarily for social purposes, a seemingly binding Constitution may risk legally binding the parties. To reduce ambiguity, it is advisable to expressly state the intention to form legally binding obligations within the Constitution or other key documents. Declaring such intention clearly in human-readable form assists legal clarity and enforcement, because smart contracts themselves are typically coded and lack inherent legibility to courts or regulators.

Smart contracts may also be coded to reflect the parties' intention. For instance, certain code provisions or logic triggers can indicate contract formation, commitment, or acceptance, serving as objective markers of intention.

Although DAOs use automated systems to perform functions without human discretion at the time of execution, this does not negate the requirement of legal intention. Rather, the law attributes the system's actions to the responsible human party, treating the system as a tool for executing their will. This attribution functions as a proxy for intention, enabling contracts formed through automation to satisfy the legal threshold for enforceability. In this way, automated systems are not seen as autonomous actors but as extensions of the human parties who deploy or authorise them.

## C. Capacity

In the context of contract law, capacity refers to the ability or legal competence of a person to enter into contracts. It ensures that individuals understand the obligations they undertake and are not unfairly exploited in the process. Most jurisdictions apply similar thresholds for measuring capacity, which is soundness of mind at the time of agreement and majority age. In some cases, additional requirements such as financial solvency may also apply, depending on the jurisdiction and the nature of the contract.

### Capacity of DAOs

Capacity to contract is not limited to natural persons. Legal entities such as corporations, LLCs, or partnerships also possess contractual capacity, allowing them to hold rights and bear liabilities independent of their members. By contrast, DAOs lack universal legal recognition. While some jurisdictions allow DAOs to register as legal entities (typically LLCs or foundations), this status is jurisdiction-specific and does not automatically confer recognition elsewhere. Consequently, even if a DAO is recognised in one jurisdiction, its members may still face personal liability in others. For unregistered DAOs, members with legal capacity can enter binding automated contracts on the DAO's behalf, but risk personal liability without the protection of a separate legal personality.

To mitigate these risks, DAOs often use legal entities to gain recognition and limit member liability. A legal wrapper fully represents the DAO as a formal legal entity. However, it risks non-recognition in jurisdictions where DAO legal status is uncertain or unestablished. Alternatively, a parallel legal entity may be used, operating independently alongside the DAO for specific activities such as contracting or asset holding. Both approaches require strict separation

of management and finances to prevent courts from piercing the corporate veil and exposing members to personal liability. Additionally, establishing entities in multiple jurisdictions can help DAOs navigate complex and varied regulatory environments.

### Pseudo-anonymity and Capacity

Another key challenge in DAO contexts is pseudonymity. The anonymous or pseudonymous nature of DAO members makes it difficult to verify whether participants meet the legal capacity requirements, such as age, mental competence, or jurisdictional qualifications needed to enter enforceable contracts or bear liability.

Privacy-preserving technologies like zero-knowledge proofs (ZKPs), which can verify personal attributes without revealing identity,[17] offer a potential solution. For instance, zero-knowledge proofs (ZKPs) can verify essential attributes (e.g., that a participant is over 18 or resides within a certain jurisdiction) without disclosing the member's actual identity. These tools help align DAO participation with legal thresholds for capacity, while preserving user privacy. However, if traditional legal systems such as courts are to be relied on for enforcement, the veil protecting privacy may be forcefully broken. Alternatively, parties may opt for an alternate means of resolution, which has the capacity to accommodate these challenges unique to DAOs.

## D. Consideration

Consideration refers to the exchange of something of value between parties, which may include money, assets, services, or even a promise to act or refrain from acting. It serves as evidence that a bargain was struck, and is traditionally a core requirement for contract formation in common law jurisdictions.

In the context of smart contracts within DAOs, the presence of consideration is often easier to identify. Transactions typically involve treasury assets, real-world assets (RWAs), or on-chain obligations recorded in immutable form. These elements provide clear, verifiable evidence of value exchange, strengthening the enforceability of such agreements.

---

[17] Anon Aadhaar is an initiative exploring ZKPs for privacy-preserving verification of Aadhaar ( Biometric and demographic ID system for Indian residents). See https://github.com/anon-aadhaar/anon-aadhaar?tab=readme-ov-file

By contrast, in civil law systems, consideration is not a necessary condition for contractual validity. Instead, the focus lies on mutual consent between parties. If consent is established, the agreement may be binding regardless of whether something of value was exchanged.

### E. Legality

For a contract to be legally binding, its purpose must be lawful and not contrary to public policy. The legality of a contract's subject matter is assessed based on applicable laws, which vary widely across countries and legal systems. For instance, *in countries where cryptocurrency exchange is prohibited, a smart contract facilitating such transactions may be deemed illegal and thus unenforceable*. Similarly, if a DAO processes personal data of EU residents via smart contracts without complying with the General Data Protection Regulation (GDPR), the agreement may be deemed unlawful, potentially exposing members to liability.

It is important for contracts to comply with all relevant laws and regulations applicable to the contract's subject matter and parties. For example, *if a DAO processes personal data of European Union residents through smart contracts without meeting GDPR requirements, such contracts could be unlawful and expose DAO participants to significant liabilities*.

Notably, the MLAC does not directly address the elements of consideration or legality. These elements must therefore be evaluated under the domestic laws relevant to the DAO's activities, whether based on the jurisdiction where the DAO operates, the subject matter of the contract, or the forum where enforcement may be sought. Given the borderless nature of DAOs, it is prudent to anticipate multi-jurisdictional scrutiny, particularly when operating in regulated domains such as financial services, data protection, or asset management.

# V. Attributing Responsibility in Automated Contracting

When a contract is formed or performed through the actions of an automated system, it becomes crucial to determine who bears legal responsibility for these actions. While automated systems execute actions with precision, they raise concerns about responsibility should be attributed. Recognising this, the Model Law incorporates a framework for attribution.

Attribution, in this context, refers to the process of linking the actions of an automated system to a person, in order to assign traditional legal responsibility. Attribution is conceptually distinct from the allocation of liability, which is not addressed in the Model Law. However, attribution may serve as a preliminary basis for determining liability under applicable laws[18]. Once an action is attributed under the MLAC,[19] it leaves the question of who is ultimately liable for any issues arising from that action to the applicable national laws, such as on contractual breach, torts, consumer protection, product liability, agency, etc.

According to Article 7 of MLAC, parties have the autonomy to agree on a procedure to attribute the actions carried out by an automated system. In the context of DAOs, this agreement may be reflected in the DAO's Constitution or in a separate contract binding on the parties. If no agreement exists, actions are attributed to the person using the automated system to perform the contract. This does not include third parties who merely operate the system, but to the person with the strongest link to the action. To objectively determine the person responsible, the Model Law considers factors such as the person who deployed the automated system, the person who exercised control over the operational parameters of the system and the action, the benefit or value derived from the action, the nature and purpose of the contract, and trade usages and practices established between the parties.[20]

In some cases, a person may use an automated system to act on behalf of another. For example,

[18]Supra note 13, at para Para 71
[19] As per Article 7 and optionally Article 8 of MLAC
[20]Supra note 13, at para Para 66

*Bill, a member of En DAO, is duly authorised to form contracts engaging service providers for the DAO's marketing and advertising purposes. He generated a smart contract with a graphic designer for a series of ten En-themed NFTs, specifying that NFT transfer to the DAO and payment for services would occur simultaneously. However, during this process, En DAO's funds got used up for other purposes. Consequently, the NFTs were transferred, but payment failed due to insufficient funds. Although this action is attributed to Bill under Article 7(2) of MLAC, it may nonetheless contractually bind En DAO, as he was acting on its behalf. However, if En DAO is not recognised as a legal entity, then Bill may be personally liable for the contract.*

The Model Law also clarifies that attribution cannot be avoided simply because the outcome was unintended. However, it provides an optional provision[21] that introduces a limited exception to this general rule. If the action produces an unexpected consequence, the other party may not rely on it to hold the first party accountable, provided that (a) the first party could not reasonably have foreseen the specific action, and (b) the second party knew, or could reasonably be expected to have known, that the first party did not foresee it. For example,

*A DAO intends to transfer 100 DAI to a Web3 charity after a majority vote conducted via a third-party platform. The platform auto-generates a smart contract to execute the transfer. Due to a non-obvious bug in the platform's code, the contract mistakenly transfers 10,000 DAI instead of 100. Since neither party could reasonably foresee the bug or its effect, the charity would be obliged to return the excess. If it fails to do so, the DAO could pursue legal action for unjust enrichment to recover the funds.*

[21] An optional provision in a model law is a section that a State enacting the law may choose to adopt or not.

# VI. Legal Enforceability of Smart Contracts in DAOs

Smart contracts offer DAOs significant advantages such as speed, transparency, automation, and reduced reliance on trust. While they excel in executing standardised digital transactions, they can also operate blindly, enforcing obligations even when circumstances make the outcome unjust or unlawful. Moreover, their enforcement capabilities are limited to subject matter that can be fully digitised, leaving many real-world obligations out of reach.

Legal enforceability bridges this gap between automated execution and legal protection. This hybrid approach retains the efficiency while ensuring that parties have legal recourse if something goes wrong, such as technical bugs, unfair outcomes, or failures involving off-chain (physical) actions. The limitations of technical enforceability, and the law's role in remedying this are detailed below.

## Limitations of Automation and Need for Legal Recourse

Smart contracts are designed to execute obligations automatically and immutably. While this creates trustless systems, it introduces three core challenges that legal enforceability helps resolve. First, many obligations arising under contracts, such as delivery of physical goods or real-world services, cannot be fully executed or verified on-chain. If parties fail to fulfill these obligations, automated systems alone cannot remedy the situation. In such cases, legal enforcement mechanisms, including court action or alternative dispute resolution, become critical to compel performance or award appropriate remedies.

Second, smart contracts can operate without discretion, which means that they may enforce obligations even when circumstances make the outcome unjust or unlawful. Conventional contracts allow parties to withhold or pause performance when fairness is in question. Smart contracts, on the other hand, execute automatically, irrespective of fairness. While some parties may choose to voluntarily correct such outcomes after execution, others may require legal intervention. Where smart contracts are legally enforceable, remedies such as restitution or compensation can be pursued through formal channels to address unjust enrichment or losses.

Third, legal intervention becomes necessary when contracts are affected by vitiating factors like mistake, misrepresentation, illegality, undue influence, or abuse of power. While DAOs often

build internal governance mechanisms to prevent such issues, bad-faith actors can still manipulate voting systems, exploit loopholes, or deceive the community through misrepresentations, such as in grant applications. Moreover, some situations cannot be addressed internally and require external recourse. Legal enforceability ensures that smart contracts remain subject to traditional remedies, such as rescission, damages, or equitable relief, even after automated execution has taken place. Consider this example:

*Imagine a DAO that runs a grant program, where members vote to allocate funds to project proposals. Alice, a DAO member, submits a grant application claiming to develop a social-good project. However, unknown to the DAO, Alice never intends to carry out the project and deliberately provides false information about her qualifications and the project's status to secure funds. She also manipulates the voting process by colluding with other members to pass her grant application.*

*Once the grant funds are disbursed via an automated smart contract, the DAO community uncovers the fraud. Given that the DAO's internal governance mechanisms were exploited and the DAO alone cannot effectively resolve the issue, some DAO members or the DAO itself can initiate legal action. They may approach a court seeking remedies such as rescission of the contract formed with Alice to unwind the grant agreement, damages for losses incurred by the DAO due to Alice's misrepresentation, and equitable relief such as injunctions preventing Alice from further misuse of DAO funds.*

### Designing for Enforceability: Legal and Technical Tools

To address these limitations proactively, smart contracts should be designed with legal enforceability in mind, incorporating both technical and legal safeguards. One essential safeguard is the inclusion of dispute resolution clauses. These may specify either on-chain or off-chain processes for resolving disagreements, allowing parties to avoid unnecessary litigation. DAOs may design custom processes for resolution, such as internal tribunals or arbitral panels composed of community members. Importantly, these mechanisms should be designed in accordance with legal frameworks,[22] so that outcomes are recognised in courts if needed.

[22]For instance, a well-structured arbitration process, if designed in accordance with national and international arbitration laws, can lead to legally binding outcomes enforceable by courts as well.

For DAOs, a key safeguard is designing fallback mechanisms that enable human or legal intervention when automation misfires. Since smart contract execution may produce irreversible results, embedding tools like time delays, pause functions, or multi-signature approvals allows members to halt or review transactions. These moments of intervention can serve as a gateway to legal recourse or internal dispute resolution before further action is taken, preserving both autonomy and accountability.

Finally, legal enforceability can be strengthened by supplementing the code with hybrid contracts that include natural-language terms. These written agreements should clearly outline the parties' rights, obligations, and remedies, and may be incorporated into the DAO's Constitution or exist as standalone documents. This hybrid model helps ensure that courts and regulators can understand and enforce the intent behind the code, making enforcement more effective, transparent, and adaptable to real-world legal standards.

## Enforcement Pathway

Designing for legal enforceability should include not just valid terms and jurisdiction, but also clear processes for enforcement. If a dispute arises, such as misrepresentation, manipulation of a DAO vote, or failure to deliver agreed services, affected parties must know how to act.

If conventional legal recourse is intended, the applicable law should be identified and followed. This law provides procedural clarity, such as how to initiate a claim, give notice, or submit evidence. For example, a party challenging fraudulent DAO governance actions must follow the procedural rules of the appropriate jurisdiction, whether specified in the contract, or, if not predetermined, determined by factors such as where the incident occurred, where enforcement is sought, or where the parties are located.

Alternatively, if parties opt out of courts and choose alternative dispute resolution, the recourse process must be adequately and expressly incorporated into the contract or supplementary documents such as the DAO Constitution. Internal processes should clearly define how disputes are raised, who decides them, and how outcomes are enforced. Clarity at the design stage helps prevent confusion and strengthens enforceability.

## Jurisdiction Challenge

Smart contracts and DAOs function across global and often overlapping jurisdictions, complicating the determination of applicable law, venue, and enforceable legal standards. These complexities highlight the importance of thoughtful legal design and international cooperation. Although detailed jurisdictional analysis is outside this paper's scope, it is essential to review applicable laws during contract design based on factors such as the location of parties, subject matter of the contract, place of performance, or where enforcement might be sought.

# VII. Conclusion

While legally enforceable smart contracts for DAO transactions will not shield participants from all legal liabilities, they strike a balance between legal protections, regulatory demands, and autonomy. Rooted in traditional contract law, legal enforceability applies only to transactions that are lawful and satisfy key contractual elements. Drawing on the UNCITRAL Model Law on Automated Contracting and traditional contract law requirements, this paper provides guidance on how smart contracts may be validly formed and performed. It also explains how they may be recognised for their role in facilitating contract formation and performance, within the DAO ecosystem. Although not expressly addressed, the Model Law may also apply to other automated/autonomous systems within DAOs, who perform these roles, such as AI agents, as they too satisfy the key criteria for contract formation and execution in this environment.

Though the Model Law is not binding, it complements existing domestic legislation and international frameworks, and embodies universally accepted legal principles. Its potential global adoption is evident from the successful adoption of other UNCITRAL model laws in shaping cross-border legal certainty[23]. This paper leverages the Model Law's foundation to help DAO participants design legally conscious smart contracts, fostering further dialogue, academic research, and legal development that clarifies automated contracting in decentralised environments.

This work is intended to support DAO designers and legal engineers seeking to create smart contracts that balance automation benefits with legal certainty and protection. It also aims to offer insights for policy makers, researchers, and stakeholders invested in building adaptable frameworks that safeguard autonomy and rights within the evolving DAO landscape.

[23]The UNCITRAL Model Law on Electronic Commerce (1996) which has been adopted by more than 80 countries worldwide is one such example. It provides a harmonised legal framework recognising electronic communications and signatures, facilitating the validity and enforceability of electronic contracts across jurisdictions.

# VIII. DAO Design Guidelines for Legal Enforceability

These guidelines are crafted to help DAO designers create better, legally informed, and protective systems. They also aim to inform all participants and external parties engaging with DAOs about potential risks and safeguards. It is my hope that researchers, developers, and DAO builders will further this work by developing and adopting these guidelines as code-based standards, enabling easier integration and promoting enforceable, and adaptable DAO frameworks.

1. **Lawful and Enforceable Subject Matter**
   Ensure the smart contract's subject matter is lawful and capable of forming a valid contract. Avoid illegal activities or those contrary to public policy. Confirm legal compliance across relevant jurisdictions.

2. **Examine Relevant Legal Frameworks**
   Assess applicable laws to identify restrictions on contract enforceability, including the legal recognition of consideration such as cryptocurrency or tokenised assets in the relevant jurisdictions. Consider factors like locations of parties, place of enforcement, and contract subject matter, to identify applicable law(s).

3. **Clarify Intention to Create Legal Obligations**
   Clearly indicate whether DAO interactions are intended to be legally binding. This can be stated in the DAO Constitution or other governance documents.

4. **Accompany Code with Natural-Language Agreements**
   Supplement smart contract code with human-readable text outlining rights, obligations, remedies, and fallback processes. This improves clarity, supports dispute resolution, and aids enforceability.

5. **Specify Applicable Law and Jurisdiction**
   Identify the law governing the contract and the resolution process, and the chosen venue (physical or virtual) for resolving disputes. Even if relying on private resolution

mechanisms (e.g. arbitration), this anchors enforceability and interpretation.

6. **Design Clear and Enforceable Private Dispute Mechanisms**
   If opting for private or internal mechanisms (arbitration, DAO tribunals), ensure the procedures are clear, and ideally lawful and enforceable as well. Include terms for initiation, process, authority, and methods of enforcing decisions (on-chain or off-chain).

7. **Establish Attribution of Actions to Legal Persons**
   Link automated actions (e.g., code execution, votes, transactions) to identifiable or pseudonymous parties. Attribution supports accountability and dispute resolution. It is ideal to agree on a process for such attribution, at the time of designing the smart contracts.

8. **Confirm Legal Capacity to Contract**
   Ensure parties interacting with contracts meet legal capacity requirements.

9. **Verify Capacity While Preserving Privacy**
   Use privacy-preserving tools to verify capacity without compromising anonymity. Consider KYC verification for age or jurisdiction, using privacy-preserving tools like zero-knowledge proofs where anonymity is valued.

10. **Minimise Personal Liability in Unincorporated Structures**
    Where the DAO lacks legal personality, design contracts and constitutions to limit individual exposure. Use sub-contracts, defined roles, or proxy arrangements to avoid open-ended liability.

11. **Consider a Legal Wrapper or Parallel Legal Entity for the DAO**
    Create parallel legal entities operating independently for specific activities like contracting or asset holding. Where feasible, use a legal entity (wrapper) to provide formal recognition, manage liability, and facilitate off-chain contracting. Also consider the incorporation of agents or multi-jurisdictional entities where necessary.

12. **Prevent Misalignment Between Code and Expectations**

    Guard against disconnects between what parties believe was agreed and what the code enforces. Supplement code with explanatory documents or comments, especially where ambiguity could lead to disputes.

13. **Embed Fallback and Human Intervention Mechanisms**

    Include features such as time delays, pause functions, multi-signature approvals, and dispute resolution processes like expert determination or mediation. These allow human review or legal intervention during automated contract execution, especially when irreversible outcomes may occur.

# Acknowledgements

Thanks to my DAOstar fellows for their generous exchange of ideas. A special thanks to Joseph for his guidance and leadership of the DAOstar Fellowship, and to Prasanth for his thoughtful feedback.

# Bibliography

1. **UNCITRAL Model Law on Automated Contracting (2024)**, G.A. Res. 79/119, Annex IV, U.N. Doc. A/79/17 (2024), available at: https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf

2. **Guide to Enactment of the UNCITRAL Model Law on Automated Contracting (2024)**, U.N. Doc. A/79/17/Add.2 (2024), available at: https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf

3. **UNCITRAL Model Law on Electronic Commerce (1996)** available at: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

4. **Nick Szabo, Smart Contracts (1994)**, available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

5. **Arizona Revised Statutes, § 44-7061 (2017)**, available at: https://legiscan.com/AZ/text/HB2417/id/1497439
6. **Tennessee Code Annotated, § 47-10-202(c) (2018)**, available at: https://legiscan.com/TN/text/SB1662/id/1802160

7. **Anon Aadhaar Project**, GitHub repository available at: https://github.com/anon-aadhaar/anon-aadhaar?tab=readme-ov-file

8. **UK Law Commission Report on Smart Contracts (2019)**, available at: https://www.lawcom.gov.uk/project/smart-contracts/

9. **The Defiant, Vitalik Buterin Criticizes Governance Tokens (2021)**, available at: https://thedefiant.io/news/defi/buterin-criticizes-governance-tokens

10. **Wright, Aaron & De Filippi, Primavera. Blockchain and the Law: The Rule of Code**. Published June 30, 2021.

11. **Wright, Aaron, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges***, *Stanford Journal of Blockchain Law & Policy*. Retrieved from https://stanford-jblp.pubpub.org/pub/rise-of-daos/release/1