Securing the Future of DeSci

William Laurent ⚡
4 min read · Apr 22, 2024

To fortify the safety of their projects, decentralized science (DeSci) DAOs are required to navigate a diverse terrain of cybersecurity measures, encompassing meticulous smart contract audits, robust hacking defenses, and the safeguarding of their governance tokens.

Considering the decentralized and frequently open-source nature of Web3 technologies and regulatory issues around personal health data DeSci DAOs are required to implement a specialized approach to cybersecurity. This journey is most effectively undertaken with the guidance of a Chief Security Officer or a top-tier cybersecurity firm.

Outlined below are three key cybersecurity areas that DeSci DAOs operating on the Ethereum blockchain must carefully address:

Advanced Smart Contract Audits

Smart contract audits are critical for ensuring the security and reliability of DeSci projects. Take care to ensure the DAO you engage with has undergone a deep and comprehensive auditing process — one that encompasses deep and wide-ranging assessments from a leader in smart contract audits.

Before an audit from the "big boys", DAO's can get started with automated testing tools such as Mythril, Slither, or Oyente, which swiftly identify known vulnerabilities like reentrancy, overflow/underflow, and gas limit issues. Additionally, integrating security measures at the design phase of smart contract development, utilizing well-established design patterns, and adhering to the Ethereum Smart Contract Best Practices Guide can preempt common pitfalls.

Following automated scans, testing conducted by experienced auditors will be essential to capture complex interactions and business logic that automated tools might overlook.

The most trusted name in blockchain smart contract audits is CertiK. Leveraging both manual and proprietary AI-driven verification methods, CertiK's audits have been instrumental in hundreds of DAOs identifying and mitigating security vulnerabilities before deployment. (Decentralized science devotees should bear in mind that AxonDAO has smartly employed CertiK to conduct a thorough review and ranking of their $AXGT smart contract.)

On a fun note, one asymmetrical strategy for bolstering security is the establishment of a bug bounty program after initial audits have been concluded. This approach incentivizes cybersecurity experts and amateurs to rigorously test contracts under real-world conditions, identifying vulnerabilities that may have evaded previous assessments. By harnessing the collective expertise of a DAO's community, such programs enhance project security while fostering a spirit of collaboration and shared responsibility.

Code Sealing, Encryption, and Digital Signatures

Code Sealing in the context of cryptography typically refers to the process of securely encrypting or digitally signing software code to ensure its integrity to safeguard against unauthorized modifications. This includes leveraging decentralized code repositories such as Radicle and standing up blockchain-based version control systems that mitigate the risk posed by centralized platforms like GitHub.

Moreover, by implementing secure hash algorithms to codebases, and storing resulting hashes on the blockchain, a foolproof seal is established, enabling swift identification of any alterations to the codebase. This involves generating unique hash values for code files or repositories, akin to digital fingerprints. Any modifications to the code will yield a distinct hash value, facilitating easy detection of tampering. Additionally, stringent access controls and meticulous change tracking within version control systems, alongside cryptographic signatures to authenticate user origin and integrity for each commit, guarantee that only authorized modifications are sanctioned. Such measures ensure that the code remains untainted during transmission or execution.

Multi-Sig Wallets

Multisig wallets, short for multi-signature wallets, require multiple cryptographic signatures (or "signatories") to authorize transactions. This means that funds stored in a multisig wallet cannot be moved unless a predetermined number of authorized individuals or entities provide their consent. This setup not only enhances security by ensuring that no single individual has unilateral control over the community's assets.

In a recent incident underscoring the vulnerabilities inherent in a crypto DAO's dependence on a single-signature wallet, the saga of Wonderland DAO stands as a stark example of what happens when a crypto project forgoes a multisig approach. The DAO found itself plunged into turmoil upon the revelation that its treasury management hinged predominantly on the actions of a solitary (and shadowy) figure, known only as "Sifu." This setup led to significant operational and governance challenges — and ultimately steep financial losses — thanks to the ability of a single bad actor to compromise the DAO's treasury.

After various financial shenanigans were discovered, the community felt betrayed by the lack of transparency and the centralized control of the treasury, which contradicted the decentralized ethos that DAOs typically stand for. This escalated to the point where a community vote was held, resulting in Sifu's removal from his position. Following his removal, proposals to either reform or wind down the project were put forward, reflecting the community's struggle to regain stability and trust. All this drama could have been prevented had Wonderland integrated a multisig wallet into its financial operations.

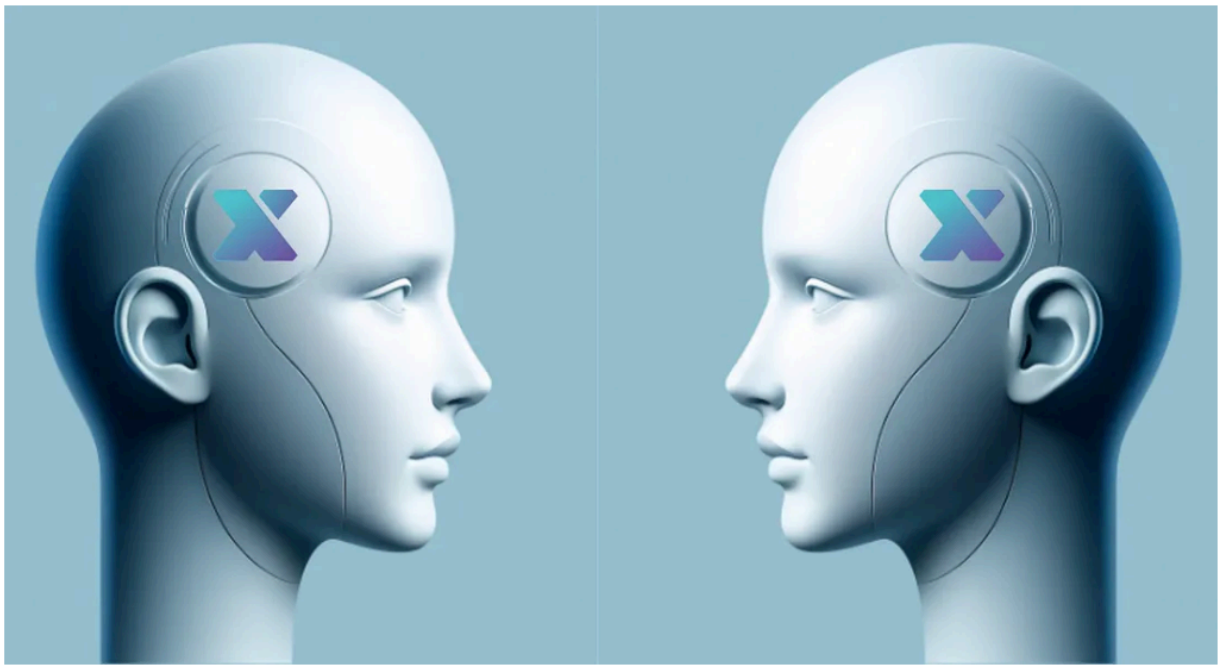
Keep the Security. Gain the Trust

Protecting a DAO and its governance tokens involves several layers of security considerations, and thus requires a nuanced understanding of both the theoretical underpinnings and practical implementations of blockchain technology. The security of smart contracts and DAOs is particularly crucial, as vulnerabilities in these areas will inevitably lead to significant financial losses and permanently undermine the trust of the community.

Given the dynamic nature of Web3, encountering hackers is an inevitability. When opting to participate in a decentralized science DAO — whether as an investor, scientist, or provider of personal health data — take great care to ensure the DAO has taken optimal measures to protect themselves and their members from the malicious activities of hackers.

Charting DeSci's Legal Course

William Laurent ⚡
4 min read · Apr 20, 2024



Big Brained DAOs incorporate in Wyoming

Decentralized Science (DeSci) utilizes blockchain technology to democratize and accelerate scientific research, breaking away from traditional, centralized control of funding, publication, and peer review. Through the adoption of decentralized autonomous organizations (DAOs), DeSci initiatives aim to bring about a new level of transparency, inclusiveness, and cooperative engagement that significantly exceeds what is currently observed in conventional scientific research practices.

Venturing into DeSci means balancing the thrill of scientific breakthroughs with the sobering complexities of law, ethics, and government regulation. It also means carefully navigating through the complexities of delicate domains like artificial intelligence, personal health data, and intellectual property rights.

To address regulatory challenges, DAOs and stakeholders need to engage proactively with policymakers and regulatory bodies. This dialogue will help shape policies that support innovation while ensuring compliance and protection for all parties involved. Additionally, adopting standardized practices for transparency, financial reporting, and governance will help DeSci DAOs build trust and credibility with both regulators and the public.

To operate with regulatory precision and be exemplary in compliance, DeSci DAOs must strategically address four key areas:

1. Intellectual Property Rights in the Age of NFTs and AI

Decentralized Science (DeSci) DAOs are exploring the use of NFTs to manage intellectual property (IP) rights innovatively. The integration of NFTs offers a way to verify and reward contributions through immutable records and automated royalties. However, the nuanced legal statuses of NFTs and AI-generated content demand thorough scrutiny. As AI begins to play a significant role in content creation, determining the rightful owner — be it human or AI — of IP becomes a complex issue that requires clear guidelines and smart contract protocols to ensure fair practice and proper revenue sharing.

2. DAO Legal Structure

The fluidity of DAOs within the legal system presents challenges, particularly regarding formal recognition, which impacts contract enforcement and liability. To navigate this, DAOs can establish a more concrete presence by incorporating in crypto-friendly jurisdictions or forming subsidiaries where laws are favorable. (AxonDAO has incorporated in the DAO-friendly state of Wyoming.) This strategic positioning aids in attaining legal recognition and addressing the intricacies of operations and IP rights within the broader regulatory framework.

3. Navigating Financial Regulations

DAOs engaging in financial activities mirror traditional institutions but often lack equivalent oversight, attracting regulatory scrutiny over concerns such as money laundering and fraud. DAOs must traverse the terrain of financial regulation with diligence, ensuring that fundraising and token issuance conform to established legal standards. This includes implementing comprehensive compliance measures to secure transactional integrity and bolster the DAO's legitimacy.

4. Governance and Decision-Making

The inherent decentralization and potential anonymity within DAOs require robust governance structures. To counteract issues of fraud and ensure responsible management, DAOs must design and enforce transparent yet secure voting and decision-making systems. These systems must adhere to legal requirements while upholding fair management practices and stakeholder engagement — a foundation critical for sustaining long-term trust and success.

Tackling these topics is of utmost importance, not only to avoid legal pitfalls but to ensure that DAOs confidently build sustainable innovation and incrementally grow stakeholder trust.

A Commitment to Conscientious Compliance

In charting a course through the regulatory intricacies of DeSci DAOs, the role of legal counsel is paramount. Retaining lawyers with specialized expertise in blockchain tech and Web3 intellectual property law is crucial if a DeSci DAO hopes to form robust frameworks and structures that stay compliant for the long term. Only get involved with DeSci DAOs that have proper legal counsel in place.

Active dialogue and collaboration with a DAO's community members are central to its prosperity. In the Web3 ecosystem, the collective voice and participation of the community are central to everything. Maintaining full transparency with the community regarding compliance and operations not only fosters trust but also attracts legally-minded contributors. Educational initiatives that inform community members about their rights and obligations can significantly reduce the risk of inadvertent legal infractions.

Finally, the adoption of Regulatory Technology (RegTech) can be a game-changer, offering blockchain-enabled automation of compliance processes. Such technology can ensure ongoing adherence to data protection and financial regulations, streamlining compliance management while minimizing human error and administrative overhead.

As decentralized autonomous organizations (DAOs) gain momentum in sectors like decentralized science (DeSci), the interplay between innovation and regulation becomes increasingly intricate. The successful navigation of this interplay is imperative for leveraging the transformative potential that DAOs offer in this emerging field.

For stakeholders in DeSci — from the researcher to the casual investor — vigilance in regulatory and compliance matters is paramount. Participants in a DAO, regardless of capacity, should conduct a thorough due diligence process. All members should be comfortable that their DAO is structured with the necessary corporate safeguards and has access to seasoned legal counsel adept at maneuvering through the regulatory frameworks pertinent to each jurisdiction of operation. Newcomers to DeSci should approach the space from a perspective of caution and educated foresight. One's participation should be marked by a commitment to conscientious compliance that matches a passion for revolutionizing the future of scientific research.