Creating an Advanced Decentralized Autonomous Organization Protocol

By Wedergarten & Jiegodose

Abstract

Understanding The History

Originally conceived in 2015, the DAO (Decentralized Autonomous Organization) was the first of its kind. It promised a system that would allow a large financial entity to be operated in a completely decentralized way, by millions of individual people across the globe, facilitated by the Smart Contract capabilities of Ethereum.

The set up was simple, deploy the code base, run a sale of ERC20 tokens which would be used for voting, and open the floodgates allowing anyone to create a new proposal to the DAO. Owners of the DAO token could then individually vote, where each token represented a vote, to form a consensus on every proposal. If a proposal is accepted by the DAO, the requested funds would then be transferred to the receiver of the proposal. Any profits created then by the receiver over time, are then cycled back into the DAO, increasing the intrinsic and speculative value of the DAO tokens.

As of today, the DAO has been the most successful way to give any cryptocurrency a tangible and intrinsic value. But, there is only one issue.

On June the 17th, 2016, the original DAO project began to be drained by an individual who was able to exploit a vulnerability in the DAO Smart Contract.

Known as a re-entrancy vulnerability, which is akin to withdrawing over and over at an ATM machine without actually updating your balance, the exploiter was able to siphon more than 3.6 Million ether into a child DAO using the “SplitDAO()” Function.

Unfortunately, this exploit caused enormous chaos within the entire blockchain community. The vulnerability could be pinpointed to a simple error where two lines of code should have been swapped, allowing the exploiter to recursively call the SplitDAO function without updating the contract. Within a few hours, the child DAO, now known as the DarkDAO, had accumulated over 60 million US dollars in Ether, which would now be valued at over 5 Billion dollars.

The following actions by the Ethereum Foundation, which resulted as a direct response to the attack, was likely some of the worst decisionmaking the internet has ever seen.

To learn more about the DAO exploit and the aftermath, please watch this video as it goes much further in depth into the entire story of the DAO exploit. What is important to understand is that the Ethereum blockchain “forked” into two separate chains in order to return the exploited funds to users of the DAO due to a vulnerability built on top of Ethereum as a Smart Contract, and not a protocol level vulnerability. As a result, we now have the Ethereum blockchain, representing the forked blockchain, and Ethereum Classic, the original blockchain.

It is up to each individual user to decide if the actions that took place were the correct moral decision in the eyes of society, but two things were made clear the moment the hard fork occurred. Firstly, the Ethereum blockchain was no longer immutable, meaning that any transaction that had been previously mined was now open to be undone or changed, therefore no longer being able to call itself immutable. Secondly, the Ether (The native currency of the Ethereum Blockchain) which was held by the attacker's child DAO was no longer worth the same as any other Ether, invalidating the fungibility of the currency.

Since this attack, Ethereum Classic has continued to be mined as the original blockchain, and never breaking any of its fundamental values. Many new DAO protocols have since been introduced to Ethereum and other blockchains. Most of them try to fix issues with their respective ecosystems, or exist to further development around the protocol.

What We Learned

By understanding the history of the DAO, we can narrow our approach to specific goals and requirements for an all-encompassing DAO. We can break it up into these segments:

Scalability:

How much can this protocol scale? To what extent can we build on top of it to support the underlying ecosystem?

Democracy:

How can we keep the fungibility of the DAO tokens while allowing for those with fewer tokens to have a larger voice, to avoid decisions not based on the majority of users but from a majority of funds?

Security:

What can we do to ensure maximum reliability for the DAO and avoid any attacks like some of its predecessors?

Stability:

How can we ensure the value of the DAO tokens when they are either being staked or locked?

Flexibility:

How can we allow users to receive the value of their DAO tokens without having to sell them at an exchange?

DAO Scalability

Understanding DAO Scalability

DAOs, like other decentralized protocols, need a built-in way to scale in order to create the capacity for other protocols to be built on top of it, assuming the goal is that the DAO in question wants to continue to be the center of power in an ecosystem. Currently, solutions to this problem have been minimal as DAOs have mostly been created as a way to earn money, and some lack the interoperability due to the constraints built into the Smart Contract. There are many factors that go into measuring the scalability of any given DAO and true scalability needs to add to each one of these factors.

We can break these individual factors down to three main arguments:

Long Term Compatibility:

Can the protocol adapt to new changes and innovations in the Ecosystem?

User base Scalability:

Can the protocol be able to support hundreds to hundreds of thousands of individual voters and builders?

Financial Scalability:

Can the protocol accept new assets over time as value to the DAO and hold them?

Using these criteria, we can now solve each problem individually and find out what, if any, conflicts exist between them.

Solving DAO Scalability

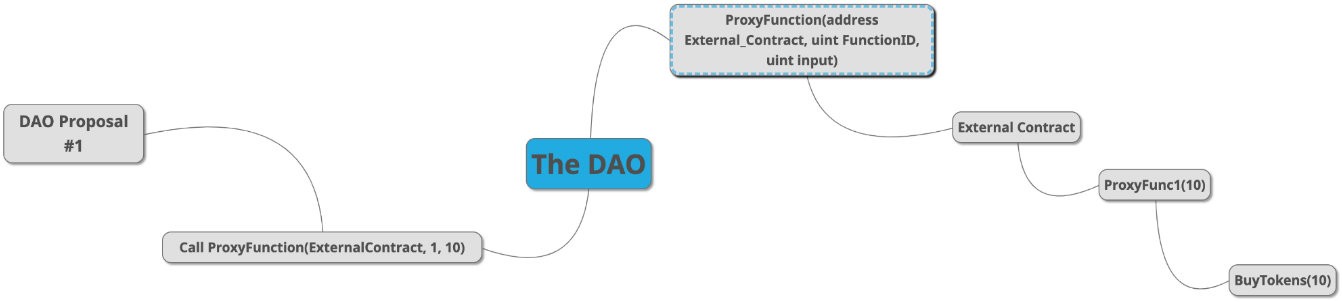
Long-Term Compatibility

In order for the protocol to have the ability to scale over time with newer technologies and protocols growing alongside the DAO, a system or a standard must be in place to ensure security while still being able to interact with other smart contracts and be interacted with by other smart contracts. Using two separate solutions, we can, to the best of our current understanding of the use cases which the DAO might need to operate create a very strong platform to be built on top of.
We'll call this the Eros standard, deriving from the name of greek god of love and compatibility.

The Eros Standard

The Eros standard consists of two implementable scalability solutions for the DAO, in which any contract can become immediately compatible with the DAO if built correctly and is approved to be used via a proposal. These implementations are a two-way street, where the DAO can call the contract, and the contract can call the DAO.

The first part of the Eros standard covers the DAO calling functions of another smart contract, using a new term, proxy functions. Proxy functions are functions that a contract that wants to be compatible with the DAO can implement, and then let the DAO know which of these functions are active. By doing this, we can create functions in a fashion similar to this schema:

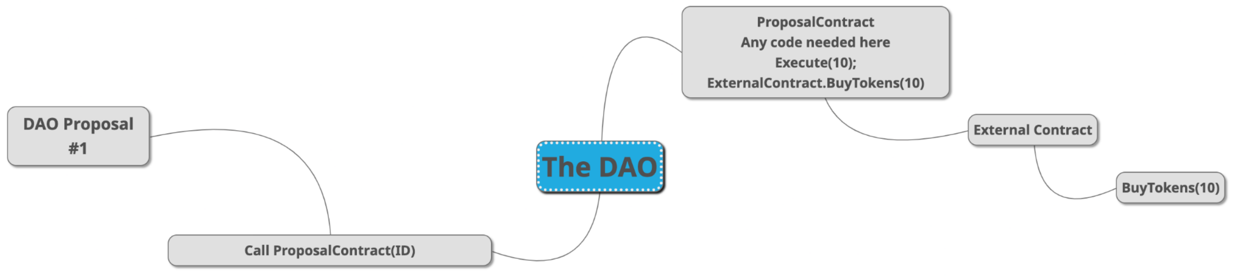

DAO Proposal #1
Call ProxyFunction(ExternalContract, 1, 10)
The DAO
ProxyFunction(address External_Contract, uint FunctionID, uint input)
External Contract
ProxyFunc1(10)
BuyTokens(10)

In this example, you can see that someone submitted a proposal to the DAO, with the ID of 1. Assuming this proposal gets executed after voting, the proposal will first call the ProxyFunction() function on the DAO contract, while providing the address of the external contract the proposal wants to call. The DAO then, using the Eros standard implementation interface, will call the ProxyFunc1() function on the external contract, which itself executes whatever code is in that function, which in this case is a BuyTokens() function, with the argument of 10 derived from the proposal.

This solution, while very efficient, has one limitation. The limitation is that certain functions on a separate contract may require a specific set of arguments, which cannot be covered by a basic system like the one above. The first part of the Eros standard will be specifically for quick attachments of new protocols, and simple governance over them.

The second part of the Eros standard is much more flexible, and may be slightly more inefficient, yet it is truly the first of its kind.

By creating a framework within the DAO contract that allows an external smart contract to be implemented directly, users or developers can create a one-time-use smart contract, with a function within it named “Execute()”, enabling completely customizable proposals that can be executed using parameters pre-determined in external code. Here's a schema to show how this structure will work:



This setup will allow for proposals to be created with arguments built right in, and become an executable function that the DAO can call through a proposal at any time.

With this solution, another problem arises. How does the external contract know that the DAO is the caller? We could try tx.origin, but that would revert back to whoever called the execute function on the DAO after the proposal was approved. Msg.sender would simply return the proposal contract, which could be anyone. Instead, we will create an "OnlyDAO" modifier that checks to see if the DAO is the message sender, or if the message sender is an approved contract in the DAO proposal registry.

By implementing both of these concepts into the Eros standard, external contracts and projects will be able to use DAO infrastructure and democracy for their own benefit until the end of time.

User base Scalability

Thanks to the flexibility of the Ethereum Virtual Machine (EVM), a DAO can be operated by hundreds of thousands of individuals for a truly decentralized organization. This DAO will be built in such a way that treats everyone equally, and voting power is only determined by the tokens that they own.

Financial Scalability

Yet another essential part of DAOs that has yet to be fully resolved is true financial scalability. A DAO must be able to accommodate many different assets at a time, so that the backing can be stable, especially in a case where an asset must be liquidated or purchased quickly. To be able to achieve this, we must implement a long-term concept that allows for the DAO to receive, send and hold many different assets.

We will begin by building a system where the DAO can decide which assets are part of its treasury, starting at a cap of five separate assets. Then, as those slots are filled, the users can decide through a proposal to increase the maximum number of registered assets as they wish. For now, the DAO will only be able to hold ERC20 assets and ether, but changes can be made with time with new versions of the Treasury contract, which can be swapped out through proposals.

The treasury, which will be responsible for holding these assets, will have infrastructure that allows those tokens to be swapped into ether or other assets through the Eros standard custom proposals. That way, the DAO can swap in and out of assets through proposals like any other user, and decide on its own holdings.

DAO Democracy

Existing Democracy

One of the core concepts of democracy is participation. Long gone are the days of the comitia populi tributa, where free citizens themselves voted directly on legislative matters in Rome. Nowadays, representatives take that role in the modern state organization. As these “elevated”, aristocratic individuals take the role of decision makers, it’s only logical that citizens take an active role in their choosing. Meanwhile, elevated discourse should be at the center of the stage.

Instead of that, we see higher levels of cynicism within external actors, internal power struggles inside the classical parties and populism taking hostage the debates that should be directed to unify the population, getting us into more divisionism in-fighting.

What has gone wrong? A lot of things could be put on the table about this matter, but the most interesting for the matter at hand of a DAO is incentives. Nowadays, participants of the democratic system don't feel/aren't actually represented. They see their leaders as the necessary evil for administering the estate's affairs, the employees that can't be dispensed as the system was not made to be run without a central body to blame for the decision making.

Enter the DAO.

Improving Democracy

In a decentralized organization, no “leader” can emerge. No “elevated” individuals, no aristocratic actors. Only participants discussing, proposing, executing.

How to focus their activity, how to set a goal post? Different solutions can be defined and different implementations could be considered, but the solutions used for this protocol are the most fair in a game where resources = power. With our locking of the voting power participants must manage their tokens to support the proposals that could benefit them the most, while allowing them to really appreciate the fungibility of the token.

As these democratic microtransactions happen, incentivizing of the proposals can make users benefit themselves while participating, all the while external (and internal) parties can make their intentions clear by promoting their projects and “sweetening the pot”. Democracy doesn't become (as it should not be) a burden, it becomes a process of discussion and solution seeking, keeping actors and participants engaged in a never-ending project of trial-and-error and improvement achievement.

Understanding Stability and Value

Another long-term and important challenge for any DAO project is the value of their token. Many rely simply on the value that the token has by being able to be used for voting, and others have stablecoin backings like DAI, or volatile coin backings, or sometimes a mix of both. Others rely simply on the speculative value of their token to continue growth. We want to use both of these to create a “Super-token” which has a little of both.

Inherited/Intrinsic Value

DAO tokens may or may not inherit value from their respective DAO protocols, as not all of them have direct value backings that can be withdrawn at any point. To make value backings count for the DAO, the representative assets that any given DAO token holds must be able to be redeemed at any time. Inherited value can take many forms, either from ether that is held by the DAO, or other tokens that the DAO holds as investments in the long-term development of the ecosystem. In the original DAO, the process to redeem the value of the tokens was a manual process that took many weeks, after splitting the DAO into your own child DAO, then waiting to create a proposal and send the tokens out. So, while theoretically the DAO tokens were directly backed by Ether, the accessibility was simply not there, and was a nuisance to token holders.

To resolve this, the Hamonia DAO protocol will have a built-in feature allowing token holders to exchange their DAO tokens and receive the backing value at any given time, for a true backing and great opportunities for arbitrage. Having this implemented also creates a true fungibility for the DAO tokens, as each one can be treated as another, both being able to redeem the same amount of assets.

Potential Value

Now, if DAO tokens are backed by inherited value, does that mean their value will always be correlated directly to the backing, and be a 1:1 representation of that value? Likely not. The reason is that while backed value may play a factor in the price of an asset, the use case that the token provides and its future potential value has a role as-well. This is why we believe that the safest approach to a long-term asset is to have a backed token with the ability to grow and fall over time as a speculative asset, similar to gold.

Tokenomics and predetermined supply

For full transparency, this protocol is meant to be built around an ERC20 token with a supply of 42 000 000 tokens, with 18 decimal points. The team or project deploying this protocol may decide how those 42,000,000 tokens are distributed over time, and how much of those will belong to their respective DAO.

Security : The #1 Priority

In an effort to prevent each and every type of attack on the DAO, we must first break down the general attack points, then ensure that the solidity code functions as we need it to, without providing any back doors into the funds or the control of the DAO.

Once the team building the DAO protocol has finished and drafted a final version and run extreme security tests and exploit attempts, onto external reviews. The plans are to get individual audits from 2 separate solidity audit companies of the highest regard, then upload the project to as many platforms as we can find that allow for bounties to be put up for bug correction, funded by us. Finally, we will ask a multitude of individual solidity experts to review our code and to try to hack it. With that, it is never possible to be 100% certain about the security of the project, but as long as the correct steps are taken to ensure maximum security, we hope to shut the door to any lurking black hat exploiters.

(This section will be updated with a full description of all tests and audits once they have been completed later on.)

Re-Inventing the DAO

Typically, society decides to improve on an existing system instead of creating a new one, and then creates solutions for each individual problem that this system has or creates, which then births additional issues within it.

A prime example would be the 2008 financial crisis, caused by a housing market that was built on credit that could no longer be held up. Instead of allowing the system to collapse, and rebuild using actual innovation, the US Federal Reserve bailed out many banks and allowed a fraudulent system to continue, and the effects of that we see today.

That is why this protocol is built specifically to dwarf the functionality and scalability of existing protocols, and to set the precedent for future development.

Conclusion

In the end, the blockchain is a straightforward and simple concept that has bloomed since 2009. Just a few years ago, the idea of decentralized finance simply did not exist, and yet today we have a very large number of decentralized applications for anything you can think of, from loans to decentralized exchanges, decentralized organizations, yield protocols, and more.

The key is that anyone, from anywhere, of any age, sex, or ethnicity can learn the concepts behind decentralized finance and payments and add to it by building further. That is why the Harmonia DAO protocol exists, to fuel passion and innovation in the best that humanity has to offer.