7.13. Fully on-chain DAOs on the Internet Computer

AUTHORS:

Björn Assman

DFINITY

Lara Schmid

DFINITY

Fully on-chain DAOs on the Internet Computer

Björn Assmann* Lara Schmid†
DFINITY Foundation DFINITY Foundation

October 25, 2023

Abstract

Decentralized autonomous organizations, or DAOs, are governance systems implemented as smart contracts on blockchains, enabling decentralized communities to make verifiable decisions on a public ledger. Early blockchains, like Bitcoin, lack built-in governance systems that we now associate with DAOs. To upgrade the blockchain, all node operators jointly agree on doing so by individually upgrading their nodes. This requires a lot of costly off-chain coordination and does not benefit from the verifiability of on-chain activities. Newer platforms like Ethereum introduced smart contracts and enabled DAOs for various decision-making processes. Typically only a few of these decisions are executed automatically on-chain and the DAO must trust off-chain individuals to do so.

The Internet Computer blockchain (ICP) addresses these off-chain dependencies through its Network Nervous System (NNS), a fully on-chain DAO that governs the entire ICP. The NNS automates all system upgrades, including those of the protocol and the NNS DAO itself. Furthermore, DAOs on the ICP control whole decentralized applications—covering their stored data, assets, and frontends.

In this paper, we detail how these fully automated, on-chain governance systems are facilitated by the ICP platform's unique design. It includes upgradable smart contracts called ”canisters”, low transaction and storage costs compared to other platforms, a distinct separation between governance participants and node operators, and protocol-embedded node upgrades.

*bjoern.assmann@dfinity.org
†lara.schmid@dfinity.org

I. Introduction

A. What is a DAO?

A governance system is a framework that allows people to jointly make decisions. The governance system defines, for example, who can contribute to decisions and how voting on decisions is organized. Decentralized Autonomous Organizations, DAOs, are governance systems that are implemented on blockchain platforms. The governance system, what decisions can be made, and what their effects are, are defined by smart contracts and enforced using software. According to some definitions [Buterin, 2014], smart contracts are only considered DAOs if they hold internal capital that they govern over.

B. A Short History of DAOs

The term DAO, and similar concepts such as Decentralized Autonomous Corporations (DACs), were introduced around 2013/2014. In 2016, a famous DAO "The DAO" was launched as a decentralized venture capital fund, where members could vote on investment decisions. A hack drained around a third of the DAO's funds, which led to a hard fork of the Ethereum blockchain as the funds were returned in one version (Ethereum) but not in the other one (Ethereum Classic). Since then, many different forms of DAOs have emerged, governing funds, full blockchains, or even real life assets. An example for the latter is the ConstitutionDAO which was formed in 2021 to purchase an original copy of the United States Constitution, but ended up losing the auction to a higher bidder [Matthews, 2021].

C. Why are DAOs useful?

DAOs are not very useful for organizations where there are few, centralized, decision makers and the decision process need not be public.

Rather they are useful for organizations where a decentralized group of people, with potentially different interests, collaborate and collectively make decisions. Since the governance rules and the decisions are encoded in smart contracts, they are publicly verifiable by all DAO members and do not require members to trust the governance system or other members.

D. The Disadvantages of Off-chain Actions

Autonomy and decentralization of trust are two central goals of DAOs. However, in many DAOs decision making satisfies these goals but the decisions are then executed off-chain. For example, the DAO decides on some protocol changes or payments to parties that are then executed by an individual off-chain. Trust in centralized parties who must execute decisions

according to what and when they are made by the DAO contradicts the aim that a DAO should be decentralized. The risk of this is illustrated, for example, by a case where ARB tokens were already spent while the respective vote was still ongoing and even had 75% of voters against it [White, 2023a]. Moreover, the fact that a DAO requires off-chain executions contradicts the goal of autonomy and has the disadvantage that the off-chain component may not be publicly verifiable. For instance, a DAO community was tricked to pay 76 ETH to an attacker who entered their wallet into a hidden row of a spreadsheet that was used to collect payments [White, 2023b].

Another kind of decision that is not executed fully automatically on many blockchains is the upgrade of the blockchain itself. Many popular blockchains, such as Bitcoin or Ethereum, are upgraded by all computers or node providers agreeing on a new protocol version and then upgrading to this new version at roughly the same time. To ensure that a blockchain is available at all times, this requires a lot of off-chain coordination.

In this paper, we present the DAOs on the Internet Computer (ICP) [DFINITY, 2022] that enable decisions that are executed fully on-chain, including upgrades of the DAOs and the blockchain protocol itself. We first present the DAO that governs the Internet Computer which is called Network Nervous System, NNS, then explain the ICP's architectural components, and finally point out distinctive features that enable the NNS DAO and other DAOs that are hosted on the ICP.

II. The DAO that governs the Internet Computer

A. On-chain Governance via the Network Nervous System (NNS)

The Network Nervous System, NNS, is the DAO that governs the Internet Computer. It is permissionless and facilitates continuous upgrades of the blockchain protocol through voting of ICP utility token holders. Unlike blockchains like Ethereum, governance is embedded and enacted fully on-chain, avoiding complicated coordination and the risk of forks. The NNS is a stake-based voting system: any ICP token holder can participate in governance by staking ICP in a "neuron" and their voting power is dependent on the staked amount. Proposals for protocol-level changes can be submitted by any ICP token holder and, upon approval through a predetermined voting threshold, are autonomously executed by the NNS on-chain. ICP token holders can vote on upgrades to new protocol versions, replacement of node machines, changes to the governance & tokenomics and much more.

B. Liquid Democracy: Inclusivity in Decision-Making

The governance model of the Internet Computer is built around a concept known as liquid democracy, that combines aspects of direct and representative democracy. For each proposal, DAO members can vote directly or delegate their voting power to trusted entities or experts. This creates a democracy where voting power is dynamically allocated for each proposal, ensuring a balance between expert input and general participation.

III. Internet Computer Architecture

A. Nodes: The Foundational Units

The Internet Computer runs on physical node machines, the foundational building blocks of its architecture. These machines execute the protocol and store blockchain state. Node machines are high specification servers, standardized for optimal performance. They are distributed across independent data centers worldwide.

Node providers are the entities responsible for the physical hardware and overall maintenance of nodes. They undergo a governance onboarding process by the NNS, which involves providing verifiable proof of identity and resources. The Internet Computer features a diverse set of many independent node providers.

B. Subnets: Striking a Balance between Scalability and Security

A subnet is a collection of nodes that run their own instance of the consensus algorithm to produce a subnet blockchain that interacts with other subnets of the Internet Computer. This concept is similar to shards on other blockchains. Subnets play a pivotal role in striking the balance between scalability and security.

- Scalability: Replication is expensive. In a system with thousands of applications that can each have a large state, it is impossible to store all this information on every single node.
- Security: Applications must run on enough nodes to guarantee data integrity and uninterrupted uptime, even in the byzantine setting where nodes can fail or be malicious.

C. Canisters: Bundling Code and State

Subnets host smart contracts, which are called “canisters” on the Internet Computer. These are computational units which bundle together code and state. Unlike on other blockchains, canister smart contracts have a range of control settings from immutable to mutable. Each

mutable canister defines a controller who can update the canister code. This allows developers to build full decentralized applications (dapps) on-chain, even if the dapps must be adjusted over time to user needs. Canisters also have the ability to make http calls and can thus be integrated with web2 components. They can also directly integrate with other blockchains.

D. Chain-Key Cryptography: Efficiency and Decentralized Security

One of the Internet Computer's key features that enable subnets is an advanced cryptographic technique called chain-key cryptography. At the heart of chain-key cryptography lies a threshold signature scheme. This scheme resembles a standard digital signature, but with a twist: the secret signing key is distributed across all nodes within a subnet. This distribution ensures that a signature can only be produced if sufficiently many nodes agree on it.

The benefits of this sophisticated cryptographic technique include:

- Consistent Public Key: When interacting with the Internet Computer, clients and dapps only need to know one root public key. They can verify messages from any subnet by using this key.
- Inter-Subnet Communication: Similarly to the clients, subnets can use chain-key cryptography to authenticate the legitimacy of the incoming messages from other subnets.
- Adaptable Node Topology: The Internet Computer's network can evolve autonomously. Nodes and subnets can be added and removed from the Internet Computer's network due to the fact that chain-key cryptography allows dynamic resharing of the distributed secret key.

E. The Reverse Gas Model: Developer and User Friendly Fueling

The Internet Computer utilizes a reverse gas model. Instead of users bearing the computational cost, developers pre-charge canisters with "cycles" by burning ICP tokens. These cycles are expended for the canister's computations and storage needs. The primary benefit of this approach is twofold: users engaging with dapps housed in canisters are not burdened with transaction fees, and they do not require specialized wallets. As a result, user interaction with dapps mirrors the experience of using traditional applications and websites.

F. The Network Nervous System's Architectural Role

The NNS DAO itself is realized by a set of canister smart contracts, situated on a special subnet. It orchestrates the organization of the entire blockchain. New node providers are approved

by the NNS DAO and are granted permission to add a limited number of nodes. The NNS DAO then determines how the available nodes are grouped into subnets. Moreover, the NNS specifies the code that is run on the nodes. When the blockchain protocol requires an update, the NNS first approves a new code version that should be run by the nodes. After that, the NNS determines which nodes should be updated to this new version, making these decisions at the subnet level.

To make this process seamless, a "registry" on the chain holds all pertinent details, including information about the nodes, their arrangement into subnets, and their respective software versions. When the NNS makes a decision, such as updating the nodes of a subnet to a new version, the protocol automatically updates this registry. Nodes then periodically access the registry, determining when to upgrade and to which version without the need for any action from node operators.

The NNS also oversees the Internet Computer's tokenomics, managing aspects such as the cost in cycles of computation & storage and token-related incentives.

IV. Internet Computer Platform properties facilitating DAOs

A. The Network Nervous System: the DAO governing the blockchain

The NNS heavily relies on the unique design aspects of the Internet Computer's Architecture.

NNS canisters are mutable smart contracts that can be updated by their controller. In order to ensure that they can only be updated according to NNS DAO decisions, the NNS canisters are set up to control each other. This design allows governance rules to evolve iteratively, adapting to the needs and optimizations of the network.

As detailed in Section III, the reverse gas model of the Internet Computer allows users to interact with dapps without incurring transaction fees. This model benefits NNS DAO members, enabling them to vote on numerous proposals at no cost. Operations on the NNS subnet are exempt from charges, ensuring that governance activities are not hindered by operational costs. This zero-cost operational model for the NNS is cross-subsidized by other subnets. This is possible due to the low computation and storage costs on the Internet Computer compared to other platforms. The affordability means the NNS can process and store a high volume of votes and proposals and also carry out decisions on the chain autonomously.

On the Internet Computer, a clear distinction is maintained between governance participants and node providers. Governance participants (ICP token holders) have the power to decide on the trajectory of the blockchain without being directly involved in its technical maintenance. Conversely, node providers, who contribute to the blockchain's stability and security, do not have influence over governance decisions, unless they become governance participants

by staking ICP and thereby becoming committed to the Internet Computer.

The Internet Computer's native capability for protocol-embedded node upgrades enables the NNS to update the protocol seamlessly without necessitating any manual steps by node operators and without the risk of forks. When the NNS approves a proposal for a protocol upgrade on a subnet, it is automatically deployed across all nodes. This automated upgrade mechanism minimizes the risk for disruptions due to operational error and maintains a high degree of network integrity and security.

B. Service Nervous Systems: System-provided DAOs

Many of the previously mentioned features that enable the NNS also facilitate other applications on the Internet Computer, including DAOs that govern individual dapps.

- Low Barriers for Governance Participation: The reverse gas model ensures that there is a low entry barrier for governance participation, as costs are minimal or even waived entirely for end-users.
- Fully On-Chain Dapp Hosting: The Internet Computer's affordability in terms of computation and storage permits dapps to be hosted entirely on-chain. This includes not just the backend but also the frontends with all their related assets. Combined with the upgradable nature of canister smart contracts, this enables dapps that are fully decentralized and DAO-controlled.
- On-chain Proposal Execution: The low costs enable all DAO decisions to be executed directly on-chain. For example, dapp canisters can be automatically updated to new code and other execution can be triggered by DAO decisions.

These advantages facilitate a variety of possible DAOs on the Internet Computer. A prime example is the built-in Service Nervous System (SNS) framework. This framework allows any dapp developer to decentralize their dapp's control by initiating an NNS proposal which launches a new SNS DAO and assigns the dapp's control to it. A successful SNS launch entails the creation of the SNS, the collection of initial funds in exchange for governance control, and the consequent transfer of the dapp's control to the nascent SNS.

In terms of architecture, an SNS DAO mirrors the NNS, featuring a stake-based governance system to facilitate decision making and governing the dapp. Moreover, it possesses a ledger that defines a unique governance token for each SNS. For easy verifiability and user adoption, all SNSs run the same canister code. However each SNS community can choose the governance rules, tokenomics, and the supported proposals according to their needs.

V. Conclusion

The Network Nervous System (NNS) DAO on the Internet Computer facilitates fully on-chain governance, including upgrades to the protocol itself. This eliminates concerns related to off-chain trust and enhances the autonomy and decentralization that DAOs promise.

Four key features of the Internet Computer's architecture empower these advancements:

- Mutable Canisters: Offering flexibility in dapp development by allowing updates to be made over time.
- Reverse Gas Model: Streamlining user interactions with dapps without the burden of transaction fees.
- Governance and Node Operation Separation: Ensuring unbiased governance, where decision-making and technical operations are distinctly separated.
- Protocol-Embedded Node Upgrades: Facilitating automatic, disruption-free protocol upgrades with increased security.

This architecture not only sets the foundation for the NNS DAO but is also indispensable for the development of decentralized applications (dapps) with canisters. Furthermore, it paves the way for the creation of DAOs that can govern these dapps comprehensively. Due to the Internet Computer's architecture, a DAO can exert full control over a dapp, including all its components such as a web frontend, and execute DAO decisions autonomously on-chain.

The Internet Computer's approach to DAOs holds the potential to redefine the blockchain landscape. Since the start of this year, more than ten SNSs have been successfully launched on the Internet Computer, raising a total of 15M USD [Lawrence, 2023]. We eagerly anticipate the evolution and future of DAOs on the Internet Computer, convinced of its potential to advance decentralized governance.

References

[Buterin, 2014] Buterin, V. (2014). Daos, dacs, das and more: An incomplete terminology guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide.

[DFINITY, 2022] DFINITY (2022). The internet computer for geeks. https://internetcomputer.org/whitepaper.pdf.

[Lawrence, 2023] Lawrence, C. (2023). Web3 platforms are successfully fundraising without a vc in sight raising $15m. https://tech.eu/2023/09/15/web3-platforms-continue-fundraising-without-a-vc-in-sight/.

[Matthews, 2021] Matthews, K. (2021). Rare first printing of us constitution sells for record $43m. https://apnews.com/article/cryptocurrency-technology-lifestyle-business-arts-and-entertainment-b0ab721a52cf20

[White, 2023a] White, M. (2023a). First arbitrum dao vote spirals into disaster: Dao rejects $1 billion spending proposal, but arbitrum already started spending. https://web3isgoinggreat.com/?tech=dao&id=first-arbitrum-dao-vote-spirals-into-disaster.

[White, 2023b] White, M. (2023b). Peopledao loses $120,000 after payment spreadsheet is shared publicly. https://web3isgoinggreat.com/?tech=dao&id=peopledao-loses-120000-after-payment-spreadsheet-is-shared-publicly.