Aragon Network

The Aragon Network is an Aragon organization that provides infrastructure and services to users of the Aragon platform, and is governed by ANT holders. The existing Aragon infrastructure enables users to create and manage organizations. Each Aragon organization exists as a set of smart contracts that define the organization's stakeholders and their associated rights and privileges. However, some rights and privileges require subjective constraints that cannot be encoded in a smart contract directly.

The Aragon Court is a decentralized oracle protocol developed and maintained by the Aragon Network. The Aragon Court can be used by organizations, including the Aragon Network itself, to resolve subjective disputes with binary outcomes. When combined with the existing Aragon infrastructure, it enables an organization to create *Proposal Agreements* that define subjective constraints on an organization's operation and can be enforced by minority stakeholders.

Aragon's Permission Architecture

Aragon organizations control which addresses have access to perform actions on behalf of the organization in a permission registry called the *Access Control List*. Addresses on the registry can be externally owned accounts or contracts. Some contracts are intended to *forward* actions based on pre-defined criteria, for example, a voting app will forward action after a successful approval vote.

By chaining multiple contracts together we can define complex criteria which constrain how actions can be performed within the organization. To illustrate this we can look at a common scenario where an organization wants to allow treasury funds to be transferred, but only if they are 1) proposed by a member of the organization, 2) approved by a majority of members, and 3) within a pre-determined budget. This can be accomplished by configuring a chain of permissions with each link imposing logical constraints on the final action as follows:

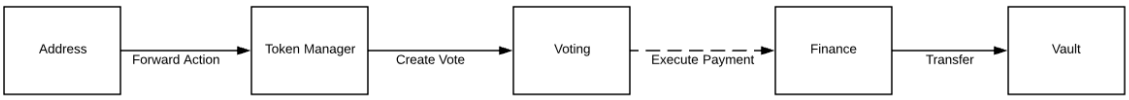

Figure 1: Token Manager --> Voting --> Finance --> Vault

The Vault, which stores the organization's assets, grants the transfer role only to the Finance application, which internally implements budgeting logic. The Finance application's *Create Payments* role is assigned exclusively to the Voting application so that the only way to create payments is to successfully pass a vote. The Voting application's *Create Votes* role is granted exclusively to the Token Manager of the organization's native token. The Token Manager will forward actions from token holders of the Token Manager's associated token.

This process effectively constrains how funds can be transferred in the organization, but the approval of a given transfer is ultimately authorized by majority vote. It's not unreasonable for a minority stakeholder to be concerned that a majority of stakeholders might decide to liquidate the organization and exclude minority stakeholders in the process.

To avoid a hostile liquidation scenario like this an organization needs a mechanism to impose a constraint that can be enforced by the actions of any individual within the organization rather than a majority of participants.

Proposal Agreements

Proposal Agreements are designed to facilitate these types of constraints within Aragon organizations. They enable an organization to define human-readable terms that proposals must conform to and require proposers to deposit collateral before their proposal can be forwarded to a voting app.

The human-readable terms can be used to protect the interest of minority stakeholders as described in the previous section, but they can also be used to define basic quality standards for what supplemental information must be included with a proposal.

Proposal Agreements can be paired with a Voting app by assigning the *create vote*, *pause vote*, and *cancel vote* roles.

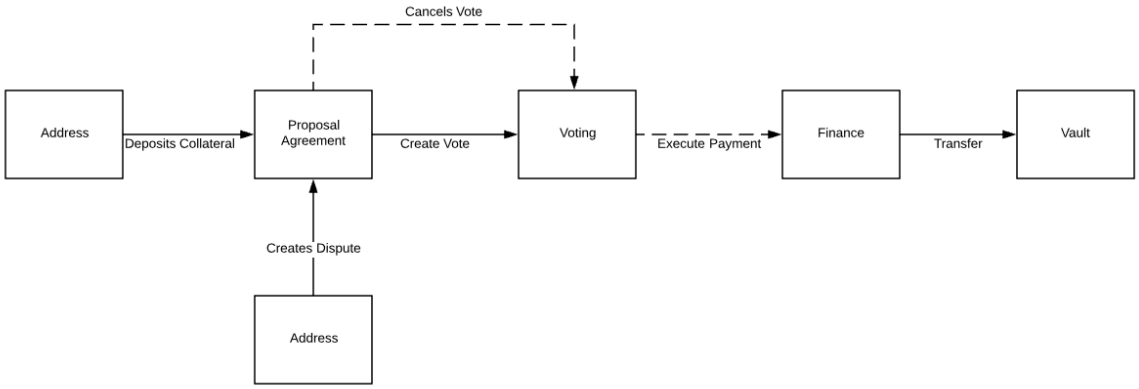

Figure 2: Proposal Agreement --> Voting --> Finance --> Vault

With this flow, when a user wants to make a fund transfer they will be prompted to review and agree to the terms of the proposal agreement.

Dispute Creation

If a minority stakeholder feels that a submitted proposal has violated the proposal agreement terms then they can choose to raise a dispute. When they raise a dispute they will need to deposit an equivalent amount of collateral, along with initial *dispute fees* as determined by the Aragon Court. They can also provide *evidence* to support their position. The vote will be immediately paused until the dispute is resolved.

If the original proposer feels that the dispute is valid then they can opt to do nothing and the dispute will be automatically ruled in favor of the disputer. The proposer's collateral will be transferred to the disputer and the vote will be canceled. If the original proposer believes they will win the dispute then they must also deposit *dispute fees* and provide evidence to support their position.

Once both parties have submitted evidence and dispute fees, the case is scheduled to be reviewed.

Aragon Court Protocol

Proposal Agreement disputes rely on a decentralized oracle protocol referred to as the *court* where *jurors* stake the Aragon Network's native asset ANT in order to earn the right to perform dispute resolution service and earn a portion of *dispute resolution fees*.

When a dispute occurs, a jury is formed by drafting jurors via *stake-weighted sortition*. Drafted jurors are required to commit to a ruling on the dispute within a commitment period, and then reveal their ruling after all drafted jurors have committed. The verdict is returned based on the majority decision of drafted jurors.

Before the verdict is enforced, there is an opportunity to *appeal*, which repeats the adjudication process with a larger set of jurors. Appeals can be made a fixed number of times before a *final judgment round* that requires every staked juror to commit to a ruling.

Juror Staking

In order to participate as a juror, an individual must acquire ANT and then deposit it into the Court's staking contract. Similar to a token bonding curve, the staking contract uses the current balance of deposited ANT to determine an exchange rate between ANT and the user's stake in the Court. Unlike a token bonding curve, we do not treat the resulting economic stake as a transferable token. This curved staking approach encourages jurors to participate early and establish the credibility of an instance of the Court, and enables the Network to deploy multiple instances of the Court protocol which compete with one another by specializing in resolving specific types of disputes.

The staking and un-staking actions are governed by the following formulas:

Staking:

Unstaking:

Where s is the resulting stake in the Court and d is the user's deposit. When un-staking, c is the amount of ANT returned. The other variables represent the state and parameters of the staking curve. r is the ratio of deposits to the total stake, b is the balance of ANT in the staking contract, and t is the total amount of distributed stake.

Once a prospective juror has staked they are considered *active* and eligible to be drafted to review cases. A distinction is made between a juror being *staked* and *active.* An *active* juror can *de-activate* themselves at any time, but they will not be able to *un-stake* until all pending disputes they have been involved in have completed.

Juror Drafting

Juror drafting is managed via a process of *stake-weighted sortition*. In order to manage the sortition process efficiently, all of the Court's operations are scheduled into *Terms*. *Terms* are defined in seconds and cannot be changed after the Court has been initialized. Terms are transitioned by calling a public *heartbeat* function which is used to make updates to *active juror stakes* from the preceding term and generate a new *random seed* for use during the subsequent term. A portion of the Court fees is used to compensate the caller of the heartbeat for gas usage.

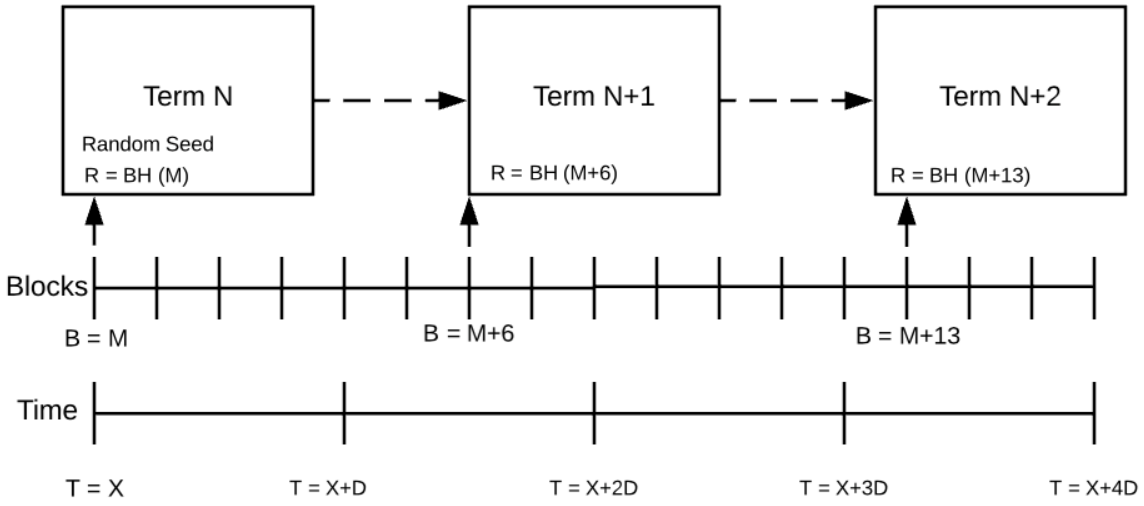

Figure 3: Court operations are broken into Terms

For each dispute or appeal we have a number of available *juror slots* that must be filled. Each slot can be thought of as a seat on the jury. A single juror can occupy multiple seats, but each seat is associated with an equal portion of their stake, which is committed and locked until the dispute is fully resolved.

One block after the heartbeat function is executed for the term in which a dispute is scheduled, a function to draft jurors for that dispute can be called. This function can be called at any point during the term and the resulting selection of jurors will be the same. If this transaction does not happen before the term ends the dispute must be rescheduled for a subsequent Court term.

To make the draft function efficient, active jurors are arranged into a tree structure based on their stake. Using the random seed for the term and the id of the dispute a random number is generated and used to traverse the tree and arrive at a juror. This process is repeated until all juror slots for the dispute have been filled.

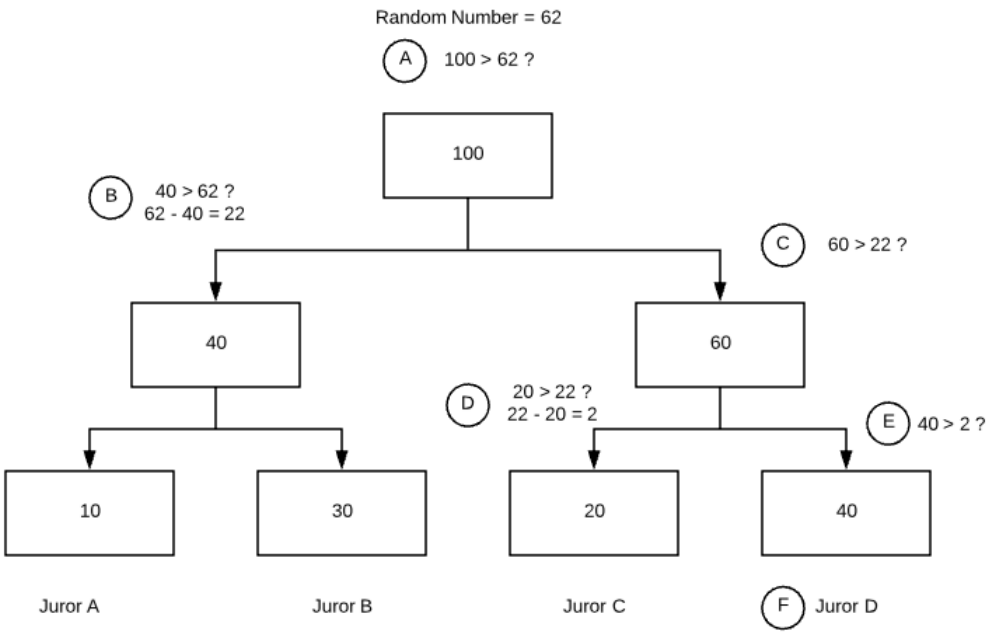

Figure 4: Traversing the sortition tree to select a juror

Due to gas constraints, the draft function can select at most 100 juror slots per call. More than 100 juror slots can be selected using multiple transactions.

Juror Ruling

Once jurors have been drafted, the dispute enters a deliberation phase where jurors are expected to provide a ruling in favor of one party or the other. Jurors are expected to make an independent judgment, but we assume that out of band communication between jurors is possible. For particularly nuanced cases there may even be forums and discussion threads used to discuss the details of a dispute. However, to minimize the ability of jurors to simply copy the voting behavior of other jurors we require rulings to be submitted in a two-phase commit reveal process.

Jurors are given a certain number of terms, called the *commitment period*, to submit a hash of their ruling. After the commit period ends, jurors are given a certain number of terms to reveal their ruling, this period is called the *reveal period*. If a juror reveals their vote prior to the reveal period, anyone can use this information to penalize the juror in exchange for a reward. If a juror fails to commit and reveal a vote by the end of the *reveal period* they are penalized.

After the conclusion of the *reveal period*, a majority of support among drafted jurors is used as a *preliminary ruling*. The preliminary ruling is considered final if there is no appeal made during the *appeal period*.

Appeals

Each dispute is subject to a maximum number of appeal rounds. Since each dispute and appeal round has a fixed duration, the maximum number of appeal rounds also determines the maximum amount of time before a final decision is reached.

Appeals can be triggered after a dispute has been resolved with a preliminary ruling in favor of one outcome or the other. In order for an appeal to occur, both sides of the dispute must deposit additional collateral. If neither side deposits the required collateral to trigger the next appeal round,

the preliminary ruling is finalized. If only one side deposits the required collateral, the ruling is immediately finalized in their favor. If both sides deposit the required collateral then the appeal round is scheduled.

The amount of required collateral depends on the appeal round and is a multiple of the fees required to compensate selected jurors. In higher appeal rounds where more juror stake is selected to adjudicate the dispute, the base amount of collateral required will be higher. The total amount of collateral required to appeal will be a multiple of this amount, 2x the base amount for the side which is reinforcing the preliminary ruling, and 3x the base amount for the side which is appealing the preliminary ruling. When the dispute is finalized the base amount is used to compensate jurors and the remainder is used to compensate the winning party for risking their appeal deposit. Appeal deposits can be crowdsourced so they do not need to be supplied by a single party.

Final Ruling

A final ruling is reached if a preliminary ruling is produced and neither side appeals, if only one side appeals, or if the maximum number of appeals are reached. When a final ruling is produced, the Court needs to process collateral and stake redistribution.

Redistributing and Unlocking Juror Stake

After a final ruling has been decided, all the adjudication rounds in the dispute can be settled. Jurors that didn't vote for the final ruling will lose the tokens that they had at stake. All the aggregated penalties and the juror fees in a round will be distributed proportionally among the jurors that voted for the final ruling option.

In case that no juror in a round voted for the final ruling, the juror tokens will be slashed and the collected juror fees for the round will be refunded to the creator of the dispute (in case that it was the first round) or to the appealing party that sided with the final ruling.

Redistributing Collateral

If there were any appeal rounds before the final ruling, the total amount of collateral that was deposited for triggering each round will be assigned to the appealer supporting the final ruling.

In the first adjudication round of a dispute (the original round created with the dispute), the Court doesn't directly manage collateral (as there may not be collateral at all or a different token is used). In cases where there is collateral at stake depending on the Court ruling, whenever the Court has a final ruling it will notify the contract being *arbitrated* with the ruling and this contract can then redistribute collateral.

Fee Summary

In order for the Court to operate fees must be captured from users to compensate jurors for their effort, risk, and opportunity cost of capital. The market for dispute resolution services exhibits some dynamics of a predator-prey relationship where the demand to participate as a juror depends on the volume of disputes, and the volume of disputes depends on the reliable presence of honest jurors.

Disputes will be rarer if there is a common expectation that the dispute resolution process is reliable and fair. The result is that as disputes become more rare, or are settled in early dispute rounds, the incentive to participate as a juror decreases. As these incentives decrease there will be less stake in the Court and it may be perceived as less reliable, resulting in more disputes and more appeals

leading to overall less consistent and efficient operation. To resolve this issue, fees are captured not just when disputes occur, but also on a recurring basis from users even when no disputes occur.

- **Subscription Fee**: A subscription fee is imposed on organizations that choose to use the Court as an arbitration provider. Subscription fees must be paid on a recurring basis for the agreement to remain valid. These fees are split between the Aragon Network's treasury and among all actively staked jurors.
- **Dispute Fee**: Dispute fees are captured at the time a dispute or appeal occurs and are calculated based on a flat amount multiplied by the amount of juror stake selected in the dispute or appeal round. These fees are distributed only to drafted jurors who rule in favor of the winning side.

This fee structure ensures that there is a consistent stream of revenue to support the operation of the Court even if disputes occur irregularly. Fees are governed by the Aragon Network organization as described below.

Governance

Governance authority over the Court is granted to ANT holders by way of an Aragon organization.

Initially, all votes will last 1 Month, require 50% Support and 1% Minimum Acceptance Quorum. Creating votes requires depositing 1000 ANT into a *Proposal Agreement* with the following terms:

Proposals must be made in good faith with the intention to improve the Network's operational efficiency, quality, or breadth of service, and benefit all ANT holders in equal measure.

The organization will face many operational decisions, including but not limited to the following:

1. Changes to the organization's permissions or the content of the proposal agreement itself.
2. Changes to Court fees and other configuration parameters.
3. Managing a treasury which is funded via a portion of the Court fees.