Aragon Network

Abstract An opt-in jurisdiction that facilitates more efficient interactions between blockchain-native digital entities using economic incentives. Users are required to stake digital assets in order to participate in governance and to collateralize subjective agreements. In the event of a dispute a decentralized court serves as an oracle to resolve and enforce agreements between participants. An algorithmic monetary policy manages reserves and issuance of ANT to incentivize participation and healthy growth of the network.

1. Introduction

The Bitcoin network has proven to be a disruptive force on the global financial system. Bitcoin's innovation is broad but the most significant contributions can be summarized as (1) combining cryptography and economics to create a novel toolkit for solving large scale distributed coordination challenges and (2) using that toolkit to secure transactions on a global peer-to-peer cash system independent of any centralized authority.

Building on the innovations of Bitcoin, Ethereum created a platform for decentralized applications that abstracts away the crypto-economic security of block production from application developers. By separating concerns, application developers can share a common security layer and thereby pool the cost of securing the network. Pooling the cost of security reduces the portion of value that individual applications must allocate to security compared to running an independent app-chain.

Ether is currently used primarily as a speculative currency, however, after transitioning to Casper proof of stake it will be used primarily to secure the network in exchange for transaction fees. Less volatile assets will become the dominant currencies used on the network. Scalability and Usability challenges will be pushed to subsequent layers through bridges and application specific side-chains, as the common platform's base-layer optimizes for cost-effective security.

The Aragon Network provides a subjective governance layer that improves the overall usability of Ethereum by providing a mechanism for pseudo-anonymous blockchain entities, including decentralized autonomous organizations (DAOs) and individuals, to create flexible human-readable agreements that are enforceable on-chain. In order to enforce an agreement on-chain, parties of the agreement must deposit collateral in the form of digital assets for the duration of the agreement. The network's native digital asset, the Aragon Network Token (ANT), utilizes a stability reserve to optimize for usage in governance of the network and as a reserve currency for collateralizing agreements.

2. Agreements {#2.0}

Enforceable agreements are a tool used to reduce friction between agents which do not trust each other. Ethereum provides one type of enforceable agreement, a smart-contract, which is enforced by protocol rules and cryptographic security. However, the types of agreements which are practical to encode in a smart-contract are limited. Smart-contracts require the terms of an agreement to be machine interpretable, do not allow for human-friendly or subjective language, and their rigidity creates a complex attack surface that is difficult and expensive to secure.

In cases where smart-contracts are not practical, agents may instead turn to traditional legal agreements. However, this poses a problem for blockchain-native agents which may not be linked to traditional legal entities. Projects like Mattereum and Openlaw are working on making it easier to link blockchain entities to traditional legal forms, but much of the censorship resistant properties that make public blockchains so valuable are lost as soon as an agent links their pseudonymous blockchain identity with their physical identity.

To resolve this tension we propose a mechanism that allows any agent to be a party to a human readable, enforceable agreement. We define an Aragon Agreement as a set of smart-contracts and a human readable document that is cryptographically signed. Aragon Agreements specify the responsibilities of relevant agents, their respective liabilities, and what mechanism will be used to enforce the agreement in the event of a dispute.

2.1 Responsibilities

Agents collaborate to define their respective responsibilities in a human readable document, similar to a traditional legal agreement, the parties of the agreement may specify their expectations for their counter-party including dates and contingencies. When both parties are satisfied with the document, it is cryptographically signed by both parties and a hash is stored on-chain. In the event of a dispute, either party may show the full agreement to another entity, that can then prove authenticity by checking the on-chain signed hash.

2.2 Liabilities

Since agreements must be enforceable without violating the security guarantees of the underlying protocol, liability for any agreement is limited to the collateral that agents deposit when creating the agreement. We assume that any digital assets can be used as collateral, and define a general interface for defining the liability of an agreement.

- **MIN_LIABILITY**: defines collateral which is exclusively locked for the duration of an Agreement. It's availability as recourse for a dispute is guaranteed.
- **MAX_LIABILITY**: defines collateral which is locked for the duration of an Agreement, but which can also be used to resolve disputes for other Agreements that share the same enforcement mechanism. Agreements which rely on MAX_LIABILITY are making a collateral efficiency/enforceability tradeoff, that enables the emergence of a robust credit system.
- **FINALIZATION**: defines EVM code that will be executed to determine whether the agreement is still valid or has finalized. Allows composability of different criteria for an agreement to finalize. Time or block spans, the ability for both or a third party to end it or prolong it are basic examples of what could be computed here.

2.3 Enforcement

Agreements must also specify an address which all parties of the agreement grant privileges to re-assign deposited collateral in the event of a dispute. This can be the address of a trusted third party, but in practice we expect that most Agreements will be enforced by the Aragon Court mechanism due to the network effects and collateral efficiency of using MAX_LIABILITY Agreements.

3. Courts

Courts are the native enforcement mechanism for the Aragon Network, they provide users with a neutral shared context for Arbitration. Each court produces an oracle feed of judgments on subjective disputes. Over time, as disputes are successfully resolved and jurors earn reputation, the judgments of a court will become more consistent as precedents are set and reinforced.

Courts are organized into a hierarchical structure, with more specific and specialized contexts at the bottom and more broad and general contexts at the top. As agents participate as jurors in a court they earn reputation in the court as well as any courts directly above in the hierarchical structure. At the very top of this structure is a supreme court that enforces and encodes the community values of the Aragon Network.

The adjudication process is structured similarly to the mechanism proposed by Kleros, however, our mechanism separates juror reputation from collateral and introduces a novel escalation metagame that makes the schelling point for jurors more resistant to bribery attacks while minimizing reliance on victims paying appeal fees.

3.1 Collateral and Reputation

We propose using collateralized agreements to bootstrap a self-reinforcing reputation system for jurors.

In order to participate as a juror in any court, an agent must agree to a code of conduct which defines their responsibilities as a juror. These responsibilities are straightforward and fulfilling them does not require a juror to depend on any other agents. A simple example of such an agreement could be summarized by the following responsibilities:

1. In the event that either party of the dispute attempts to bribe the court, the juror agrees to flag the case for review.
2. In the event that both parties attempt to bribe the court, the juror agrees to vote for dismissal of the case.
3. In the event that a single party attempts to bribe the court, the juror agrees to rule in favor of the party which did not attempt to bribe the court.

The purpose of this agreement is to create a metagame with a Nash equilibrium that favors honest jurors over malicious agents and dishonest jurors attempting to influence court decisions.

The network can set a MIN_LIABILITY agreement for jurors collateralized with ANT, and in exchange grant juror a baseline reputation within a court. As the juror participates in disputes within the court honestly and effectively, they will accrue additional reputation. This mechanism is designed such that anyone can get reputation by collateralizing agreements, but the cost to earn reputation through honest participation is significantly cheaper.

When a new court is initialized, there will be a small amount of reputation relative to collateral, but overtime as the court adjudicates disputes the proportion of reputation relative to collateral will increase. As the court matures, this transition makes it less and less cost effective to influence the rulings of a court by purchasing and staking collateral.

Since reputation is court specific and non-transferrable it is more difficult to sell, however, even if reputation within a court is sold, the impact of an individual court becoming compromised is minimal. Honest jurors within the court can organize to fork the court keeping their reputation balances, and parties of agreements enforced by the court can mutually agree to use a different court.

3.2 Adjudication Process

We assume that a client side application will be used by all participants to monitor on-chain changes and alert them when actions are required. This includes being selected for a jury, dispute initialization, appeals, and ultimately resolution.

Jurors who are willing to actively participate in arbitration within a court activate their reputation in order to be eligible for selection on a jury. When a user triggers a dispute they must pay an arbitration fee proportional to the amount of reputation that will be included on the jury. A jury is formed by randomly selecting from all activated reputation within the court at the time of the dispute.

Once the dispute is initialized and the jury formed, the adjudication process is broken up into four time windows, the duration of each can be different depending on the specific court being used:

- **Evidence Submission**: a period when parties of an agreement can submit statements and evidence to the jury.
- **Jury Ruling Period**: a period for jurors to review submitted evidence and submit a ruling. The ruling determines if the case should be (1) escalated for review, (2) dismissed, (3) have the Agreement's FINALIZATION parameter updated and/or (3) whether collateral should be reassigned between parties.
- **Ruling Review Period**: a period which is triggered if atleast one juror flags the case for review, the evidence and jurors rulings are reviewed by a second set of jurors selected from the Review Court. The review process is intended to punish jurors who do not self-report bribery or vote in such a way that is not coherent with the jurors code of conduct.
- **Appeal Period**: a period after the court has provided a ruling, but before reputation is assigned to participating jurors.

3.2.1 Jury Ruling

The Jury Ruling mechanism operates as a schelling point game where jurors individually assess the evidence and make a ruling and have an incentive to rule along with the majority of other jurors.

Since a ruling must aggregate input from all jurors, the following procedure is used to create a jury ruling and reward participants.

1. If a majority of the jury indicate the case should be dismissed, then the case is immediately dismissed, with no changes to the agreement.
2. If a majority of the jury indicates that the Agreements expiration should be extended, then the expiration is extended by the median value of those juror votes. If no appeal is made, than jurors who voted for extending the expiration earn reputation, and those that did not vote for extending the expiration lose reputation.
3. If a majority of the jury indicates that collateral should be re-assigned then collateral is re-assigned based on jurors voting on a new collateral ratio between the two parties and taking the median value. If no appeal is made, than jurors who voted for re-assigning the collateral earn reputation, and those that did not vote for extending the expiration lose reputation.

4. If no appeal is made Fees are distributed to all jurors regardless of whether they gained or loss reputation.
5. If any juror flags the dispute for review, before the court proceeds with a ruling the evidence and jury's ruling is reviewed.

3.2.2 Ruling Review

The Ruling Review mechanism assesses if any jurors violated their Juror Agreement and removes them from the adjudication process before the court provides its ruling. It operates under the assumption that for a given jury if there is at least one honest juror who flags a dispute we can punish all dishonest jurors.

If atleast one juror flags a case for review we automatically select 5 jurors from the Review Court, a court that is specifically used for evaluating if other jurors have complied with the Juror Agreement. Since this court only handles cases which have been flagged for review, participants do not need specialized knowledge about the case, they just need to assess whether the Jury complied with the Juror agreement. Reviewed cases have only 3 possible outcomes for the ruling: the dispute was flagged incorrectly and the original ruling is served, dispute was flagged correctly and the case is dismissed because both parties attempted to bribe the jury, or the dispute was flagged correctly and ruled in favor of the party that did not attempt to bribe the court.

If any of the jurors are found to have not complied with the juror agreement by the reviewers they will lose all of their reputation and their collateral will be assigned to the Networks Stability Reserve, unless they choose to appeal.

3.2.3 Fees

Jurors are compensated for their time reviewing disputes through arbitration fees. Fees are set at the court level and can be governed by reputation holders within the court. The network also sets a base fee for all court handled disputes which is directed to the network treasury. This fee is used to help support future development of the network and to compensate jurors who participate in the Ruling Review process when applicable.

3.3 Appeals

Any party which is unhappy with ruling made by the court has the option to appeal during the Appeal Period. We require an appeal to double the reputation weight of the jury, this means doubling the fee of the original dispute or most recent appeal. By requiring the jury pool to increase for each appeal we ensure that parties do not simply appeal multiple times hoping for a favorable jury, but rather each time they appeal they are sampling from a larger portion of active jurors and therefore giving the ruling more authority.

If there is not enough active jurors within the court, we can select jurors from courts from higher levels in the court hierarchy, eventually pulling in every active juror in the supreme court to produce a decision which can no longer be appealed. In practice we expect the cost to escalate a dispute to that level would be prohibitive in all but the most extreme cases, but it is important that the option to escalate disputes is available.

4. Reserve

Agreements require agents to lock up collateral, in some cases for extended periods of time. If a highly volatile asset like ETH is used, parties of the agreement are exposing themselves to the volatility risk of the collateralized asset. On the other hand if a stablecoin like DAI is used both parties face an opportunity cost of holding an asset that has no upside potential. The ideal currency for collateralizing agreements would provide competitive risk adjusted returns for holders and frequently split to ensure it can still be used as a stable unit of account. It would also retain some of its utility while locked up.

To optimize ANT for usage as a reserve currency for agreements and minimize the opportunity cost of participating in governance of the Aragon Network, we propose a monetary policy that programmatically manages both the supply of ANT and a stability reserve based on a price target. In addition, to encourage participation and long run growth of the network we incorporate a participation rate target, inspired by Livepeer, that diverts a portion of inflation to reward specific groups of users who actively contribute to growing the value of the network. Using inflation to reward positive contributions to the network is similar in principle to the coinbase rewards in Bitcoin and Ethereum.

This approach to creating a low volatility currency is closest to the work being done by Fragments, but is also inspired by Maker, StableUnit, and Basis. As research in this area matures, we expect that there will be many low-volatility currencies available with slightly different risks, rewards, and utilities that lead to their adoption as the preferred medium of exchange and store of value for specific communities. Within the Aragon Network jurisdiction, the marginal utility and rewards of participation in governance will lead to ANT becoming the preferred reserve currency for collateralizing agreements.

4.1 Price Feed Oracle

Agents can agree to act as price feed oracles by collateralizing an agreement with ANT that commits them to provide accurate price information and not attempt to manipulate the results of the feed. We can take the median value from all participants weighted by their collateral to get a price for a specific period.

If an agent tries to manipulate the price feed, a dispute can be created and the agent's collateral taken. Since price information is widely available and fairly objective, this mechanism should provide reasonably strong guarantees under the assumption there is at least one honest agent monitoring the price feed.

Agents which provide the price feed take on risk by collateralizing an agreement and must be compensated both for that risk and for providing a service to the network. A portion of inflation is dynamically allocated to incentivizing this behavior based on a target level of participation.

4.2 Stability Reserve

The purpose of the stability reserve is to dampen the volatility of ANT, particularly on the downside, in order to ensure that it can be effectively used as a unit of account and store of value for collateralizing agreements. By optimizing for store of value and unit of account properties, it is likely that ANT could also become a common medium of exchange.

As the demand for ANT grows and prices rise, ANT is minted and sold to collateralize a reserve. When prices fall the reserve automatically sells collateral in order to buy ANT and remove it from circulation. If there is insufficient collateral in the reserve to buy ANT and maintain price targets, bonds can be issued to support the price and paid back by the network at a later date. Unlike other bond mechanisms, the Network's ability to pay back bonds in the future is not strictly tied to appreciation of ANT, but also from revenue generated by services provided by the network such as the Court.

If there is sufficient collateral in reserve, defined by a stability threshold parameter, ANT can split in order to maintain a stable unit of account while ensuring that holders of ANT benefit from network value appreciation.

4.3 Price, Stability, and Participation Targets

The monetary policy of ANT is intended to be mostly algorithmic, automatically responding to changes to price and participation rates to promote the healthy growth of the network. In order to respond to these variables the algorithm must be parameterized with a set of target values for price, stability, and various participation rates.

Changes to these parameters can be constrained so that adjustments must be made in small increments and significant changes would need to be done gradually over a long period of time.

4.3.1 Price Target

The price target determines when the supply of ANT is expanded or contracted. For simplicity of implementation this could be set to a common unit of account like the USD, but ideally would be set to an inflation adjusted basket of goods similar to the CPI. Targeting a specific currency requires little intervention, whereas, targeting a basket of goods or basket of currencies requires the network to manage the elements and weights of the basket.

4.3.2 Stability Target

The stability target determines how conservative the automated reserve policy is. With a high stability target the reserve will hold more collateral, however, as a result holders of the currency will experience less value appreciation through currency splits. It is likely that the optimal stability target will change over time as the network and currency grows and becomes inherently more stable.

4.3.3 Participation Targets

Participation targets are used to incentivize important contributions to the network including maintaining a desired ratio between collateralized and liquid ANT, rewarding price feed providers, rewarding dispute reviewers, and funding the treasury. In general participation targets look at the ratio of ANT collateralized for a specific purpose relative to the total supply.

For example, if the network wants 75% of ANT locked as collateral and 25% to remain liquid we can set the participation target for collateralized ANT to 75%, then for a given period if collateralized ANT is below the target more of the value from inflation is directed to participants with collateralized ANT, conversely if the amount of collateralized ANT exceeds the target, less of the value from inflation is directed specifically to participants with collateralized ANT. This is beneficial because it allows the network to encourage the use of ANT as collateral, while ensuring that there is a pool of liquid ANT that can be held by market makers.

5. Governance

Governance is about coordinating groups and making collective decisions. As the size of the group and the number of required decisions grows, governance becomes increasingly difficult. Often the aggregate preferences of a large group diverge from the preferences of individual constituents, and each individual constituent cannot effectively process and participate in all the decisions that are made. The result is a tension between scaling decision making capacity, and ensuring that decisions are representative of the aggregate preferences of the group.

For the Aragon Network to be successful as a global jurisdiction, its governance process must increase social scalability relative to alternative jurisdictions by minimizing the trust, effort, and direct involvement necessary for participants to benefit from its operation.

5.1 Principle of Least Authority

Rather than one monolithic structure, the Aragon Network can be separated into components, each with varying degrees of influence on the network, if a specific component has a large and immediate impact on the network, the governance processes associated to it must be highly authoritative. Similarly if there is a component that does not need to be changed, then it should be static. There are four primary components of the Aragon Network ordered from most significant to least significant.

- **Upgradability**: The ability to upgrade contracts that constitute the Network. Granting authority to upgrade contracts is a superset of all other privileges and therefore should require the highest possible authority.
- **Courts**: The ability to arrange the court hierarchy, and set arbitration fees at the court and network level. Courts are used to enforce agreements within the network, significant changes to the structure and fees of courts should require significant authority.
- **Monetary Policy**: The ability to manage price feeds, stability targets, and participation targets that govern the supply of ANT and the stability reserve. These parameters are critical to the stable growth of the network, but changes are constrained such that the impact of any single action is minimized.
- **Fiscal Policy**: The ability to direct discretionary funds held in the Network's treasury. Since the treasury is isolated from the Network's Stability Reserve, governance of discretionary funds will have limited short-term impact on the network.

5.2 Stakeholder Representation

Actions that require high authority, such as upgradeability, should ensure that all stakeholders have some way to check the power of other stakeholders. In the case of an upgrade of the Aragon Network we should consider: users of agreements, ANT holders, and Jurors. While the exact processes for governance of network upgrades has not been defined and will ultimately be decided through a series of experimental deployments, a reasonable process that incorporates checks and balances would look something like this:

1. ANT holders vote to propose an upgrade
2. Reputation holders in the supreme court vote to approve the proposal
3. A wait period is enforced before the upgrade occurs that allows parties of agreements to mutually decide to use a different arbitration mechanism, or simply settle their agreement.

5.3 Incentivization

Every participant benefits from good governance but the effort and opportunity cost of actively contributing leads to minimal participation and poor social outcomes. This is a classic free-rider situation, where the benefits are shared among everyone in the network, but the burden is not widely distributed.

Attempts to resolve this issue by incentivizing participation in governance can have unintended consequences, for example paying people to vote will increase voter turnout but does not necessarily result in voters fairly considering all options and voting responsibility. Futarchy, in theory, does an excellent job of aligning participation incentives so long as there is an objectively measurable outcome to optimize.

However, in the absence of a measurable outcome we can use collateralized agreements and the court mechanism as a general primitive for incentivizing participation in governance that generally aligns with the values of a community. In order to participate in certain aspects of governance we can require agents to collateralize an agreement with ANT, committing them to a specific code of conduct. In the event that a decision is made that violates the code of conduct, such as voting for a proposal to send all treasury funds to participants who vote to approve the proposal, anyone can pay an arbitration fee to raise a dispute and put the offending parties collateral at risk. In exchange for taking on the risk and putting up collateral, the network can use monetary policy to incentivize participation without encouraging participants to vote in a malicious or negligent way.

6. Conclusion

We propose the Aragon Network, an opt-in blockchain native jurisdiction, as a means to improve social scalability in the blockchain ecosystem without requiring users to give up their privacy and freedom by associating their physical identity with their blockchain identity. Economic incentives are used to create a self-reinforcing subjective oracle for enforcing human readable agreements and resolving disputes. Since the network does not rely on physical identities to enforce agreements users are required to collateralize their agreements with digital assets, which can be highly inefficient compared to traditional jurisdictions. To minimize capital costs of collateralized agreements, the networks native digital asset ANT is designed to be an efficient and practical reserve currency that retains its primary utility, governance, even while used as collateral.