WE'RE WATCHING YOU NOW
Aragon is a project to empower freedom by creating tools to enable decentralized governance.
World's best currency for economic development
SOON™
The Architect, v0.5 Beta

Assets
- Source code (zip)
- Source code (tar.gz)
Unstoppable Organizations

Create value without borders or intermediaries
## Opened Votes

<table>
<thead>
<tr>
<th>TIME REMAINING</th>
<th>QUESTION</th>
<th>TOTAL VOTES</th>
<th>PROGRESS</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 D 23:58 M 14 S</td>
<td>Should we fund disaster relief for victims of hurricane Irma?</td>
<td>33.33%</td>
<td>✓</td>
<td>View Vote</td>
</tr>
</tbody>
</table>

## Closed Votes

<table>
<thead>
<tr>
<th>STATUS</th>
<th>QUESTION</th>
<th>TOTAL VOTES</th>
<th>RESULT</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Token Manager (ngo): Mint 1 tokens for 0xC43B0C4b6d227536238f071fb7e624b2A632830</td>
<td>50%</td>
<td>✓</td>
<td>View Vote</td>
</tr>
<tr>
<td>Approved</td>
<td>Should we help reimagine democracy in the United States of America?</td>
<td>50%</td>
<td>✓</td>
<td>View Vote</td>
</tr>
<tr>
<td>Approved</td>
<td>Finance: Create a new payment of 753 BCC. It will be executed 1 times at intervals of 0 days</td>
<td>50%</td>
<td>✓</td>
<td>View Vote</td>
</tr>
<tr>
<td>Approved</td>
<td>Token Manager (ngo): Mint 1 tokens for 0x15bdCb665f5a5e9Cef07b2a981dd270BA505051</td>
<td>100%</td>
<td>✓</td>
<td>View Vote</td>
</tr>
</tbody>
</table>
### Token Balances

<table>
<thead>
<tr>
<th>Token</th>
<th>Amount</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCC</td>
<td>26</td>
<td>$340,358.69</td>
</tr>
<tr>
<td>ETH</td>
<td>3.14</td>
<td>$1,613.52</td>
</tr>
<tr>
<td>ZRX</td>
<td>453</td>
<td>$319.01</td>
</tr>
<tr>
<td>DNT</td>
<td>137</td>
<td>$9.26</td>
</tr>
<tr>
<td>ANT</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>MANA</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>SPANK</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>SNT</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>MKR</td>
<td>0</td>
<td>$0</td>
</tr>
</tbody>
</table>

### Transfers

<table>
<thead>
<tr>
<th>Date</th>
<th>Source/Recipient</th>
<th>Reference</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/04/18</td>
<td>0x61D463f2613F04053bc875C72aA9dA22348Da2b5</td>
<td>Food aid</td>
<td>-753 BCC</td>
</tr>
<tr>
<td>13/04/18</td>
<td>0x39a4D265db942361D92e2B0039ca73Ea72a2ff9</td>
<td>Requested airdrop (test tokens)</td>
<td>+453 ZRX</td>
</tr>
<tr>
<td>13/04/18</td>
<td>0x772080b0D48Da808dbE0F4050083B0f9205F6D29</td>
<td>Ether transfer to Finance app</td>
<td>+3.14152 ETH</td>
</tr>
<tr>
<td>13/04/18</td>
<td>0x39a4D265db942361D92e2B0039ca73Ea72a2ff9</td>
<td>Requested airdrop (test tokens)</td>
<td>+137 DNT</td>
</tr>
</tbody>
</table>
Opened Votes

- **Question:** Should we fund relief for victims of hurricane Irma?
  - **Total Votes:** 33.33%

Closed Votes

1. **Status:** Approved
   - **Question:** Token Manager (ngo): Mint 1 tokens for 0xC4380C4b6d227536e23890708a7ee24b2A632830
   - **Total Votes:** 50%
2. **Status:** Approved
   - **Question:** Should we help reimagine democracy in the United States of America?
   - **Total Votes:** 50%
3. **Status:** Approved
   - **Question:** Finance: Create a new payment of 753 BCC. It will be executed 1 times at intervals of 0 days
   - **Total Votes:** 50%
4. **Status:** Approved
   - **Question:** Token Manager (ngo): Mint 1 tokens for 0x15cd6b65f5a5e9Ceo072a89810d2708A505051
   - **Total Votes:** 100%
DOM

Wrapper UI

App UI

JS
Time to take a deep dive!
DOM

Wrapper UI

App UI

JS

UI Framework
Aragon.js server
Cache
Msg handler
Web3
Messenger

UI Framework
Aragon Client
Messenger

EVM

aragonOS

Kernel
ACL
EVM Scripts
App 1
App 2
App 3
Introducing aragonOS 3.0 alpha, the new operating system for protocols and DApps

Smart contract codebase has been frozen, audit with WHG starts today and announcement for Aragon v0.5 release schedule
aragonOS
aragonOS

A framework for programming governance

github.com/aragon/aragonOS
Out of the box

1. Upgradability
2. Complex permissioning
3. Transaction forwarding
contract DelegateProxy is ERCProxy {
    uint256 constant public FWD_GAS_LIMIT = 10000;

/**
 * @dev Performs a delegatecall and returns whatever the delegatecall returned (entire context execution will return!)
 * @param _dst Destination address to perform the delegatecall
 * @param _calldata Calldata for the delegatecall
 */

function delegatedFwd(address _dst, bytes _calldata) internal {
    delegatedFwd(_dst, _calldata, 0);
}

/**
 * @dev Performs a delegatecall and returns whatever the delegatecall returned (entire context execution will return!)
 * @param _dst Destination address to perform the delegatecall
 * @param _calldata Calldata for the delegatecall
 * @param _minReturnSize Minimum size the call needs to return, if less than that it will revert
 */

function delegatedFwd(address _dst, bytes _calldata, uint256 _minReturnSize) internal {
    require(isContract(_dst));
    uint256 size;
    uint256 result;
    uint256 fwd_gas_limit = FWD_GAS_LIMIT;

    assembly {
        result := delegatecall(sub(gas, fwd_gas_limit), _dst, add(_calldata, 0x20), mload(_calldata), 0, 0)
        size := returndatasize
    }

    require(size >= _minReturnSize);
/**
* @dev Performs a delegatecall and returns whatever the delegatecall returned (entire context execution will return!)
* @param _dst Destination address to perform the delegatecall
* @param _calldata Calldata for the delegatecall
* @param _minReturnSize Minimum size the call needs to return, if less than that it will revert
*/

function delegatedFwd(address _dst, bytes _calldata, uint256 _minReturnSize) internal {
    require(isContract(_dst));
    uint256 size;
    uint256 result;
    uint256 fwd_gas_limit = FWD_GAS_LIMIT;

    assembly {
        result := delegatecall(sub(gas, fwd_gas_limit), _dst, add(_calldata, 0x20), mload(_calldata), 0, 0)
        size := returndata.size
    }

    require(size >= _minReturnSize);

    assembly {
        let ptr := mload(0x40)
        returndatacopy(ptr, 0, size)
        // revert instead of invalid() bc if the underlying call failed with invalid() it already wasted gas.
        // if the call returned error data, forward it
        switch result case 0 { revert(ptr, size) }
        default { return(ptr, size) }
    }
}
Permissions

Access Control List (ACL)

```solidity
interface IACL {
    function initialize(address permissionsCreator) external;
    function hasPermission(
        address who,
        address where,
        bytes32 what
    ) external view returns (bool);

    /* Non-interface suggestions for implementations:
    function createPermission(address who, address where, bytes32 what) external;
    function grantPermission(address who, address where, bytes32 what) external;
    function revokePermission(address who, address where, bytes32 what) external;
    */
}
```

Interface: https://github.com/aragon/aragonOS/blob/dev/contracts/acl/IACL.sol
Implementation: https://github.com/aragon/aragonOS/blob/dev/contracts/acl/ACL.sol
Permissions

Using the ACL: auth()

```solidity
/**
 * @notice Create a new vote about "_metadata"
 * @param _executionScript EVM script to be executed on approval
 * @param _metadata Vote metadata
 * @return voteId Id for newly created vote
 */

function newVote(bytes _executionScript, string _metadata) auth(CREATE_VOTES_ROLE) external returns (uint256 voteId) {
}
```
Transaction Forwarding
Transaction Forwarding

We’ll get to it.
Let’s make some governance happen!
contract DAOFactory {
    function newDAO(address root) public returns (Kernel) {
        Kernel dao = new Kernel();
        dao.initialize(root); // Assume this also creates an ACL for the DAO
        return dao;
    }
}
contract DAOFactory {

    function newDAO(address root) public returns (Kernel) {
        Kernel dao = new Kernel();
        dao.initialize(root); // Assume this also creates an ACL for the DAO

        ACL acl = ACL(dao.acl());

        Vault vault = Vault(dao.newAppInstance("vault"));
        Voting voting = Voting(dao.newAppInstance("voting"));
        Finance finance = Finance(dao.newAppInstance("finance"));
        TokenManager tokenManager = TokenManager(dao.newAppInstance("token-manager"));

        acl.createPermission(finance, vault, vault.TRANSFER_ROLE());
        acl.createPermission(voting, finance, finance.CREATE_PAYMENTS_ROLE());
        acl.createPermission(voting, finance, finance.EXECUTE_PAYMENTS_ROLE());
        acl.createPermission(voting, tokenManager, tokenManager.MINT_ROLE());
        acl.createPermission(voting, tokenManager, tokenManager.ASSIGN_ROLE());

        return dao;
    }
}
Core design tenets

1. Primitives-focused
2. Default to opt-in
3. Interchangeable, malleable components
Moving back up the stack...
Toolkit for Aragon applications, including:

1. Messaging
2. Transaction forwarding
Sandbox RPC

↔ events
↔ call
↔ intent
↔ cache
→ notification
← context
Action (Vote) → App UI → Aragon Client → Messenger

→ Wrapper UI → Aragon.js server → Msg handler → Web3

→ App Script → Aragon Client → Messenger → Cache

EVM
Script

EVM

Event (Vote)
Aragon Client

Messenger

Aragon.js server

Msg handler

Web3

Messenger

Cache

EVM

New state
## Transaction Forwarding

**Sign Transaction**

- **Permission note:**
  You cannot directly perform this action. You do not have the necessary permissions.

- **Action Requirement**
  Here are some options that you can use to perform it:
  - **Voting (ANT)**
    - The Voting (ANT) app will create a new voting for ANT holders to decide whether to perform this action or not.
  - **Tokens (XVT) → Voting (ANT)**
    1. The Tokens (XVT) app will forward actions requested by XVT token holders.
    2. The Voting (XVT) app will create a new voting for ANT holders to decide whether to perform this action or not.

**Action to be triggered**

This transaction would eventually perform a payment to address 0x52b11ka11

**Sign Transaction**
And finally back to the DOM...
Aragon UI allows you to develop apps that look and feel like Aragon apps.
A real DAO, in use, right now
Aragon Package Manager

Web 3.0 package manager for arbitrary content:
- Smart contracts
- Websites
- Docker repos
- Git repos

with pluggable Aragon governance
Aragon Package Manager

Web 2.0 bridge:

aragonpm.com -> aragonpm.eth

testtest.rinkeby.aragonpm.com
Aragon Package Manager

- **DAO ACL app**
- **Kernel**
- **DAO main address**
- **APM DAO**
- **APMRegistry app**
- **ENS Subdomain Registrar app**
- **Repo app**
- **Voting app**

- `acl()` function
- `kernel()` function
- `createName('voting')` function
- `voting.aragonpm.eth` pointed to repo
- `Deploy repo instance and assign permissions` function
- `Create 'voting' repo` function
- `Create 'voting' repo` function
- `Create voting.aragonpm.eth v2` function

- 'Kernel' relationship means app uses the Kernel for access control and upgradeability
Hack guides coming soon™!
Looking ahead
Applause from Alberto Elias and 104 others

Luis Cuende
Project Lead @AragonProject, Cofounded & Advisory Board @StamperyCo, @Forbes 30under30, HackNow Winner. Former Advisor to the VP of the EU. Freedom lover
Feb 14 · 5 min read

Decentralizing Aragon’s development
Splitting the Foundation from the core devs, and kickstarting funding for other teams to work on Aragon
Introducing Aragon One
The first company contributing to Aragon's development
Community

- 8,000 members @ aragon.chat
- 20,000 token hodlers
- 60,000 twitter followers
Come hang out!
aragon.one
aragon.chat
github.com/aragon
Hiring

- React, UI Engineers (fulltime + contractors)
- Developer Relations (fulltime)

wiki.aragon.one/jobs
Aragon Nest
Aragon is a project to empower freedom by creating tools to enable decentralized governance.
Aragon - The fight for freedom

https://www.youtube.com/watch?v=AqjlWmiAidw