White Paper v0.1

BoardRoom: A Next-Generation Decentralized Governance Apparatus

By: Nick Dodson

With the rise of new decentralized consensus technologies such as: Bitcoin and Ethereum, the demand for a reasonable blockchain governance apparatus has greatly increased. Organizations will want a secure apparatus to both simulate and activate organizational decision making on the blockchain. Organizations that include, but are not limited to: Incorporated companies, decentralized autonomous organizations (“DAO's”), decentralized corporate organizations (“DCO's”), and non governmental organizations (“NGO's”) etc., will all need governance apparatus to successfully integrate themselves into decentralized smart-contract and consensus ecosystems. What BoardRoom aims to provide is an apparatus that enables organizations to fully integrate their top and low-level managerial structures and decision making into the Ethereum consensus system so that they can potentially leverage any technically feasible contractual service or asset through democratic assembly.

Technical Overview

The BoardRoom apparatus is a decentralized application that will involve a contractual back-end largely supported by Ethereum's consensus system and a lightweight client-side interface for it's front-end. While there are multiple ways to implement BoardRoom, this document will only fully envision one possible way of designing the apparatus. BoardRoom will also leverage Ethereum’s Whisper (a decentralized and encrypted communication protocol) and Swarm (a decentralized and encrypted file-storage protocol).

Core Contractual Properties and Structure

The core BoardRoom contract will act as the central back-end for the apparatus. The contract can be either a collection of contracts with one central hub (a hub and spoke implementation) or one central contract (a rigid implementation). The core contract should contain, but is not limited to, the following properties:

1. A member system to add and remove members
2. A proposal system to table proposals
3. A democratic voting system to establish agreement or disagreement (i.e. board consensus) on tabled proposals

4. An electable chair to split even or undecided votes
5. A budget and fund allocation system
6. A subcommittee system to add and remove subcommittees
7. A parent or executive board property
8. Proposably alterable properties
9. A suicide property, to allow the board to be democratically destroyed
10. Extendability to other smart-contracts through contractual hooks
11. Extendability with other smart-contracts through contractual communication
12. Special member permissions properties

All core BoardRoom contract properties, as listed above, should only be alterable or executable, post deployment, through democratic assembly.

Members

If a user deploys or is a member of a BoardRoom contract, they will be allowed a set of possible options to interact with BoardRoom. BoardRoom members can:

1. Table new proposals
2. Vote on proposals
3. Execute winning proposals
4. Change their account address
5. Resign from the board
6. Delegate their vote to another member

Each board member is assigned a numeric identification number. This allows members to change their address.

Board members may also be given the ability of a special permission. A member with special permissions can complete one or many specific board room tasks, such as, adding in a member, without the requirement of board consensus each time. However, members may only be given special permissions by democratically established consensus of the board.

Handling Rogue Members & Compromised Member Accounts

Two potentially harmful scenarios for the boards using the BoardRoom apparatus are (1) rouge members and (2) compromised accounts. Here is an account of each of these potentially harmful scenarios and how the board can address both of them democratically through BoardRoom's proposal system:

(1) A rouge board member is an individual that, for whatever reason, is given access to the board as a board member but does not participate or behave in a way that is productive to or in the good interests of the board. This includes but is not limited to behavior such as: spamming the board with false or useless proposals or spamming communication channels. In order to deal with rogue members, the board can table a proposal to have the member removed.

(2) A compromised member is a member that's local Ethereum account's have been stolen, or are under a third-party's control without the consent of the member in question. In order to deal with compromised member accounts, the board can table a proposal to have the member accounts address changed.

Proposals

BoardRoom is a proposal based governance apparatus. The core contract should contain a proposal system in which proposals can be tabled and voted on by board members. Proposals should, at the very least, have the following properties:

1. A name or comment data store
2. An address data store
3. An uint data store
4. A bytes32 data store
5. A uint count of the current sitting members
6. A ledger to track who has voted
7. A boolean to mark if the proposal was executed
8. A rigid type designator
9. A timestamp to mark proposal creation

Proposals are executable if they have won consensus in with the sitting board members. If consensus is established, the proposal has been won and can be executed. Any member can choose to execute successful proposals. Executing the proposal entails transacting with the core BoardRoom contract. While the member who chooses to execute a proposal will be charged the gas cost, methods could be developed to bill the board for these costs and pay the member back the required gas cost.

Proposals are strictly typed, and have 13 available uint operand codes (“types”). The operand codes are as follows:

1) Send Funds

This opcode is used to send funds to a specific address. In order to send funds an address and value must be specified in the proposal. Also, if the value specified exceeds the budget, then the funds will not be sent and the proposal will be marked as executed.

2) Add Member

This opcode is used to add a member to the board. A valid address of the member must be specified.

3) Remove Member

This opcode is used to remove a member from the board. A valid member ID must be specified in the proposal.

4) Change Chair

This opcode is used to elect a new chair. A valid member ID must be specified in the proposal.

5) Add Subcommittee

This opcode is used to add a new subcommittee to the board. A valid address must be specified in the proposal.

6) Remove Subcommittee

This opcode is used to remove a subcommittee from the board. A valid committee ID must be specified in the proposal.

7) Set Parent Board

This opcode is used to set the parent or executive board. A valid address must be specified in the proposal. Note, the parent board has executive powers of it's children.

8) Outward Bytes32 Call

This opcode is used to complete an outward bytes32 call to a specific contract. A valid address of the contract must be specified and the bytes32 data can be optionally set.

9) Outward UInt Call

This opcode is an outward uint call to a specific contract at a specific address. A valid address of the contract must be specified and the uint data can be optionally set.

10) Suicide Board

This opcode is used to delete or suicide the current BoardRoom contract. No specific proposal data is required other that the type operand code.

11) Change Member Permission

This opcode is used to change or give a member a special permission. The member address must be specified and a valid opcode value is required.

12) Change Member Address

This opcode is used to change a board members address. The address provided must be a valid and not empty. Board members may propose to change their own address which will result in a proposal that, by default, is won.

13) Set Configuration Address

This opcode is used to set the configuration address of the core BoardRoom contract in use. An address is optionally required as the board may choose to nullify the configuration address.

14) Middleware Transaction

This opcode is used to make a formal outward middleware transaction to a specified middleware contract. A valid middleware contract address is required and transaction value can be optionally specified. This will make an outward transaction with the only data being the respective proposal ID.

Voting

With the BoardRoom apparatus, tabled proposals are voted on by the sitting board members. Each member of the board is given one vote. Members may choose to delegate their votes to other members. Members may only vote on proposals that were created after the time at which they joined the board. Members may only delegate votes to other members for proposals that were created after they joined the board. In an even vote, the chair member will split the undecided vote.

Boards can change the winning ratio of proposals, from it’s default 6/4 to whatever ratio suits the board. Voting weight may also be changed to reflect a different system than just democratic voting (i.e. one member one vote), equity holdings is one example, where the board votes are weighted on the bases of equity shares held in the company.

Transitioning Boards

Boards may want to transition their assets, funds and membership to another boardroom contract. There are two approaches to completing this operation. (1) Boards, with trust, manually transition all membership, funds, assets and ownership to another board. This would be done by proposal, until everything is moved over to the new contract. (2) The second option would be to allow third-party membership middleware access to the board, whereby all available funds, membership and so forth would be moved over in one complete set of contractual operations. In this scenario, a board would only have to agree on a proposal to bring in the member middleware, and then propose to activate it. This could potentially allow the smooth transition of boardroom funds, assets and membership from one board to another.

Parent or Executive Boards

The BoardRoom apparatus supports parent or executive boards which hold ultimate and executive power over their children. A parent board can table proposals that always win in their respective child boards. A parent board also has the executive power to decide what proposals win in their child boards as whatever proposal they vote for, will immediately be won. One example use case of parent boards are majority shareholder scenarios, where a majority share holder has ultimate power to do as they wish over the boards they have control over (in other words, anything they want, goes). Any proposal a parent board votes against does not pass and cannot be won by the child board. Parent boards are set either by proposal or upon construction of the BoardRoom contract. If the parent is set by construction (i.e. contractual deployment), only the parent board can change the parent address. If the parent is set by election, it remains changeable by democratic consensus of the respective child board. The proposal to set the parent board must contain a valid address of the parent board. A member will be added, if not already, for the parent board to allow it voting, tabling and execution access.

Subcommittee's

The BoardRoom apparatus supports subcommittee's. Board's can add and remove subcommittee's. Adding a subcommittee to a board gives no additional powers to the so-called parents. Only democratic consensus from the child board or a preset parent board

can do that. However, adding subcommittee's does establish that the so-called parent board maintains through democratic consensus that a specific set of boards are the subcommittee's of their board. The BoardRoom apparatus will provide an interface to test whether the subcommittee's are either actually or representational subcommittee's of the board as only actual subcommittee's would set their parent board to the board that is testing it. Subcommittee's can be added by proposal. The proposal must contain a valid address of the subcommittee.

Compromised Parent Boards

There is a possibility that the parent or executive board could be compromised. In this case the child subcommittee's could potentially be at risk, as parent boards hold executive powers over their children. In this case, the subcommittee could, if the parent board is elected, nullify the parent board temporarily and thus mitigate their risk exposure from the compromised parent board. However, if the parent board was present upon deployment, then the respective subcommittee's have little to know option to mitigate their risk from the rogue parent board.

Rogue or Compromised Subcommittee's

There is a possibility for a subcommittee to be compromised or go rogue from it's parent parent board. A subcommittee could go rogue by nullifying their parent board and refusing to set it's parent board back the legitimate parent. This would allow the subcommittee to take the assets and services available to it, and do as they wish with them, without the possibility of the parent board intervening.

In order to prevent this, subcommittee's can be deployed with a preset parent board. In this case, only the parent board would be able to change the address of the parent for it's respective child boards that have allowed it ultimate access. However, this approach leaves open the possibility that a compromised parent board could hold ultimate power and the subcommittee would leave the child board with no way to respond to this threat. This must be considered when deploying a board with a preset parent. Allowing the subcommittee's to elect their own parent boards allows them to nullify the parent boards temporarily if a parent board is compromised. This adds both additional benefit and risk and must carefully decided before deployment or board initiation.

Organizational Structures That Can Leverage BoardRoom

BoardRoom can be used in multiple circumstances with various kinds of organizational structures. All of these organizational types could leverage BoardRoom to simulate, mirror, activate and discover organization decision making on the Ethereum blockchain. Here is a list of possible organizational structures that could leverage BoardRoom, the list is as follows:

1. Decentralized Autonomous Organizations (“DAO's”)
2. Decentralized Corporate Organizations (“DCO's”)
3. Incorporated Company's
4. Non-profit Organizations (“NGO's”)
5. Trusted Third-Party Auditors
6. Governmental Organizations

Middleware

One important aspect of BoardRoom will be the ecosystem of middleware contracts that will be built around it. BoardRoom middleware merely interprets outgoing board communication and transactional data from a given boardroom and reinterprets said data to fit the required needs of other contracts and services within the Ethereum ecosystem. It is highly recommended that middleware keep an ownership ledger and that multiple BoardRooms be able to use the middleware service at anyone time. Some potential use cases of middleware contracts with Boardroom are, but are not limited to:

1. Starting a crowdfunding campaign with specific data
2. Payout out the company budget to multiple accounts (i.e. company payroll)
3. Sending tokens or digital assets to an exchange
4. Registering a name
5. Buying or selling digital assets
6. Interaction with other Boards
7. Member equity share management
8. Translational apparatus to move one board to another

Middleware Design

Middleware for BoardRoom can be built in multiple ways, all of the middleware types below aside from General Hook Middleware are only activated through executing proposals that have won, the middleware types are as follows:

1) General Hook Middleware

This form of middleware is attached to the config address as a hook contract on the central BoardRoom contract. When proposals are tabled, executed or voted on the hook contract is called with a specific set of data. This is much like Gaven Wood's Config contract hooks found in multiple examples throughout the Ethereum decentralized app repository (i.e. 'Dapps Bin').

2) Fund Recipient Middleware

This form of middleware is activated by listening for funds from a specific boardroom. Once the funds are sent from a specific address the middleware is activated.

3) Call Recipient Middleware

This form of middleware is activated by a bytes32 or uint call from a specific boardroom contract. Once the call is made to the constructor of the contract, the middleware is activated.

4) Proposal Specific Hook Middleware

This form of middleware is a bi-lateral transactional approach to middleware. The middleware will support a specific method that receives one variable, the proposal ID, and whatever funds are bound with the transaction. The middleware will have access to BoardRoom proposals as all board proposals are publicly accessible, and so all proposal data related the proposal in question will be available to the middleware to use. This kind of middleware established a specific proposal based two-way approach to middleware for boardroom. I maintain that this is the most flexible, adaptable and approachable way to design and build middleware for BoardRoom.

5) Member Middleware (API Access)

This form of middleware uses the BoardRoom member system to grant third-party services API access. A board can vote in a member that is addressed to a contract instead of person. This would allow the board to grant API access to a third-party service. Essentially granting the middleware board member privileges. Member middleware can be given a special permission through the BoardRoom permissions system. An example use case of member middleware would be, fee based board membership access. Member middleware can be designed so that it is limited in functionality. Some member middleware will only be able to table proposals while other may be granted access to bring in new members, or send funds.

Please note, that this list is not fully encompassing and that other BoardRoom middleware designs are possible.

Amendments

Using standardized BoardRoom middleware, proposals can be linked to others contractually. This can be used to create an amendment structure, whereby proposals, ruling or decisions can be amended to update further changes or modifications.

A Walk Through of Multiple Case Uses of BoardRoom

Listed below are a few example case uses and walkthroughs of BoardRoom in action:

1) Fund Allocation (Payroll) via Middleware

A board wants to allocate funds out of the board budget to several specific addresses. One member enlists the help of contractual middleware and sets specific amounts to be delegated to specific addresses. A proposal is tabled to delegate the total amount of funds to the middleware. The board reviews the middleware contract to ensure it is secure and trusted. The proposal is then voted on and passes. The funds are then delegated from the board budget too the middleware contract. From there they are delegated to the addresses specified above.

2) Crowdfuding via Middleware

A board wants to start a crowdfunding campaign to raise funds for their board or company. A member then enlists the help of contractual middleware and set's up the specific date required to start a crowdfunding campaign with the beneficiary address set to either the board or company account. A proposal is then tabled to call the specific middleware contract with a specific data key that will begin the crowdfunding campaign. The proposal is voted on and passes. The proposal is executed and the call is made to the middleware to start the crowdfunding campaign. All beneficiary funds will be sent to specified company or board account.

3) Adding a Subcommittee

A board decides they want to create a new subcommittee for their community outreach program. A member then deploys a BoardRoom contract with a specific chair address specified in the constructor of the contract. The member then tables a proposal to add the subcommittee with the new committee address specified in the proposal. The board votes and

the proposal is won. The proposal is then executed and the subcommittee is added to the verified subcommittee roster.

Whisper Integration

The Ethereum infrastructure provides a secure and encrypted decentralized messaging and communication protocol called Whisper. BoardRoom can leverage whisper by allowing secure communication between boards (i.e. parent or subcommittees) and board members. A Whisper discussion topic can be assigned for each proposal, and an intuitive Whisper interface can be integrated into the BoardRoom apparatus.

Swarm Integration

The Ethereum infrastructure will also provide a secure and encrypted decentralized file-storage protocol called Swarm. Swarm's file-storage protocol can be leveraged by the BoardRoom apparatus to support secure inter-organizational communication. Proposals, for example, could be paired with hosted files on Swarm which would allow board members to securely share files that only board members can access. An intuitive file-sharing interface will be integrated into the BoardRoom apparatus.

Espionage Mitigation

Integrating Whisper and Swarm into BoardRoom will provide a high degree of security for organizational communication. This will aid organizations in preventing corporate, governmental and inter-organizational espionage by reducing the chance of communication leaks that would otherwise be present with more conventional communication technologies (e.g. email, Skype, or Dropbox).

While communication channels may be private, all BoardRoom consensus data points are public as they leverage Ethereum's public consensus system. So BoardRoom boards would not be able to hide what funds are sent where, however, boards could hide nearly every contextual aspect of their consensus activities. In order to achieve this, an encryption system could be leveraged to encrypt all proposal, board and member context data, such as names, with key based encryption methods. The key could be delivered securely to sitting members through a decentralized communication protocol such as Whisper upon members joining the

board, and only members given a key would be able to locally unlock the relevant context data of the board.

As well, BoardRooms could choose not to leverage a public name registration contract, which would largely keep their activities private.

Configuration Hook's

The core BoardRoom contract contains a configuration address that will be called only if the configuration address is set and is valid. A validation should be put in place in order to establish that the config contract is healthy and active. The configuration contract is called every time a new proposal is tabled, voted on or executed.

If a configuration address is bad and a validation system is not present, the board's proposal, voting and execution system can be disabled as any of these actions by board members would result in an infinity high gas prices.

In order to address this potential problem, a validation process should be established to see if the configuration contract exists and is healthy before the transaction to that contract is made. If this validation system can not be technically established, then the chair should be able to override the config address so that the board can continue normal operations.

If a bad configuration address is present, and a configuration validation system is not, then the chair could hold the board hostage, by continuously preventing funds or normal board activities from continuing. This hostage scenario would be rare, however, it stresses the need for a configuration validation system to vet and test that the contract is working before an outward call is made to the configuration contract.

A Multi-Contractual BoardRoom Design

Another possible contractual design for the BoardRoom core contract is one where the core leverages multiple contracts to make up the critical functionality of the BoardRoom contract. The proposal, member, subcommittee and democratic voting systems may all be voted on by the board and could be subject to change. Initially, the BoardRoom contract would be setup with default and trusted contracts. One benefit of building BoardRoom in this fashion is that the board can vote in new or updated critical BoardRoom systems that follow the same interface structure. A board may want to vote in a new member system or proposal system, with this design, this is possible. One possible negative of this design pattern is that if a board mistakenly votes in a contract that is badly designed, fraudulent, or non-existent, it may risk

the board's health and security as critical functionality may no longer be accessible.

Conclusion

The BoardRoom apparatus will provide a stable, dynamic, adaptable, democratic, open-ended, multi-purpose and secure voting system that will enable groups and organizations with the necessary tools to leverage the full potential of Ethereum's decentralized consensus ecosystem through democratic assembly.

Further Reading

Buterin, Vitalik. (2013). Ethereum White Paper.
<https://github.com/ethereum/wiki/wiki/White-Paper>

Buterin, Vitalik. (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/>

Dietz, Joel. (2014). Distributed Governance Whitepaper.
<https://github.com/fractastical/distributed-governance/blob/master/whitepaper.md>

Dahlstrom, Dana; Shanks, Bayle. (2009). Software Support for Face-to-Face Parliamentary Procedure.
<http://odbook.stanford.edu/static/filedocument/2009/11/15/Chapter_18._Dahlstrom_and_Shanks.pdf>

Leblanc, Richard; Gillies, James. (2005). Inside the Boardroom: How Boards Really Work and the Coming Revolution in Corporate Governance. Wiley;

A. Dhir; Aaron. (2015). Challenging Boardroom Homogeneity: Corporate Law, Governance, and Diversity. Cambridge University Press.