PENN BLOCKCHAIN

Blockchain Governance and DAOs

Alex Miao

(Loosely based off a talk by Jake Brukhman)

Overview

Motivation and Background

Blockchain Governance Case Studies

- Bitcoin
- Ethereum
- Tezos

Ideas in Blockchain Governance

- Fred Ehrsam
- Vlad Zamfir
- Vitalik Buterin

DAOs

Ideas in Voting

- Banzhaf Index
- Quadratic Voting

Motivation and Background

Motivation

A blockchain project needs to be updated with patches, bug fixes, new features, etc.

But, the code is currently being used by thousands to millions of people, and not everyone likes the update

How do we decide what changes to make?

Motivation

Some blockchain projects are run by companies. They reach a decision internally and update the software.

But, many blockchain projects are not companies because they don’t want centralization risk. So, there are many different ways in which they can make decisions

Blockchain Governance

Governance decisions need to happen at multiple layers of the technology stack, and decisions interact with each other.

Layer 1 - What type of Proof-Of-Stake algorithm should Ethereum use? Should Bitcoin transactions have a segregated witness?

Layer 2 - Should we implement submarine swaps in lightning?

Storage Layer - Should we update IPFS?

Application Layer - What collaterals should MakerDAO allow as for CDPs?

Blockchain Forks

Bitcoin and Ethereum are protocols, meaning that they define message structures and expected behaviors for how nodes interact

Nodes have to run software that implements this protocol, and there can be different versions of software running within the network

Ex. go-ethereum vs cpp-ethereum

Blockchain Forks

Soft fork - a new version of software that is backwards compatible

Hard fork - a software update that is not backwards compatible

- Need to copy everything on to new chain

Voting on Blockchains

Blockchains allow for secure, decentralized voting in which votes are tallied

Basic Commit-and-Reveal Scheme:

1. Commit Phase - individuals encrypt vote and timestamp with with some key, send to smart contract
2. Reveal Phase - after everyone votes, individuals send key to smart contract, which tallies votes

There are fancier voting schemes that allow more anonymity in voting, different voting models, etc.

Liquid Democracy

Blockchains are secure and decentralized so we could write a voting contract that allows people to delegate voting power to others.

If you disagree with how a delegate votes, you take back your delegation

Basis for many Proof-Of-Stake systems

Blockchain Governance Case Studies

Bitcoin Governance

3 main groups of people who interact with the network

1. Users - increase individual holdings, increase functional utility of network
2. Miners - own hardware to mine blocks and get mining rewards
3. Developers - write code that miners and nodes have the option of running

Developers write code, but it’s up to miners if they want to adopt new software

Miners incentive is to maximize earnings, leads to centralization and ASICs

Ethereum Governance

Similar to Bitcoin: Ethereum users, miners, developers

But we have ecosystems of DApps running on Ethereum, each with own demands

Ethereum Foundation - Non-profit that gives out grants and voices opinion on Ethereum development

Consensys - Private company that develops and funds development of DApps on Ethereum

Core Developers - Group of programmers that make most Ethereum implementation decisions

Tezos Governance

Brief introduction to Tezos

Layer 1 Protocol

Liquid Proof-Of-Stake

- Bakers - Nodes with 10,000 XTZ Stake that vote on blocks, earn inflation
- Users delegate XTZ to bakers and earn inflation for baking

Michelson smart contracting language

- Functional, Formal verification

Tezos Governance

On-chain governance - Developers individually submit code to Tezos blockchain, then on chain vote takes place

Done to prevent forking the protocol, once a majority is reached, everyone updates code

Takes power away from developers and miners and gives it to user

Tezos Governance

Tezos hard fork - disagreement between Tezos Foundation and OCamlPro

Tezos Foundation threatened to stop funding Tezos development by OCamlPro for not making all of their software open-source

OCamlPro decided to hard fork the Tezos blockchain

Ideas in Blockchain Governance

Ideas on Governance

A series of 3 articles published in late 2017 in response to each other addressing the problem of blockchain governance

Fred Ehrsam - Thesis

“Blockchain Governance: Programming Our Future”

Two components of governance: incentives and coordination

Blockchains allow us to formalize rules through smart contracts

We can design systems to align group incentives and coordinate decision making

Fred Ehrsam - Thesis

Futarchy - Prediction markets are used to determine governance decisions

Members of society vote on a scale of 0 to 1 how satisfied they are with the year.

Form predictions market on what the average will be for next 100 years.

Before a decision is made on a bill, markets will speculate based on how societal welfare changes as a result of the bill

Let the market decide which policies are best

Vlad Zamfir - Antithesis

“Against on-chain governance” published in response to Ehrsam’s article

“Blockchain governance is not a design problem”

You haven’t successfully solved the governance problem until people actually adopt it and use it readily.

Governance is a process where participants continuously learn about each other and update their state of knowledge. There are many norms and conventions in how people interact

Vlad Zamfir - Antithesis

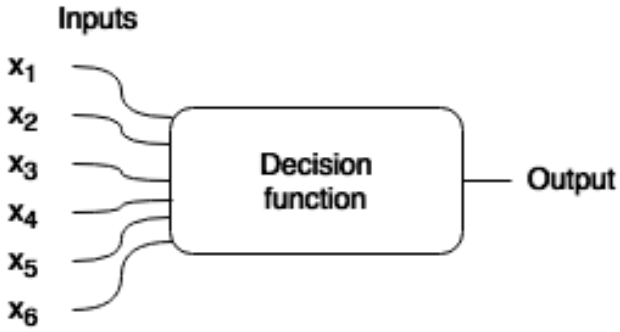
A shift to fully on-chain governance is a “revolution” but we really just need incremental improvement, do not need on-chain governance at layer 1 (but perhaps at smart contract level)

Node operators fall to “default” decided by on chain decision process, and become disenfranchised

Vitalik Buterin - Synthesis

On-chain governance is overrated

Governance as a decision function vs coordination game - decisions are not independent



	A	B
A	(5, 5)	(0, 0)
B	(0, 0)	(5, 5)

Vitalik Buterin - Synthesis

On chain voting (coin voting) has really low voter turnout

Coin holders are only a single class of user

HODLers vs users

Game-Theoretic Attacks

Probability voter has impact is small: “And if each person's size of the stake is small, their incentive to vote correctly is insignificant squared. Hence, a relatively small bribe spread out across the participants may suffice to sway their decision, possibly in a way that they collectively might quite disapprove of.”

Digital constitutions are bad because they are not expressive enough

DAOs

DAOs

Decentralized Autonomous Organization

Difficult to define, but loosely is a collection of people who make decisions that are tied to financial incentives through smart contracts

Examples of DAOs

MAKER

MolochDAO

Started out to fund ETH2.0 development

Started in February 2019

Inspired by “Meditations on Moloch” blog post by Scott Alexander.

> The dictatorless dystopia:
>
> “Imagine a country with two rules: first, every person must spend eight hours a day giving themselves strong electric shocks. Second, if anyone fails to follow a rule (including this one), or speaks out against it, or fails to enforce it, all citizens must unite to kill that person. Suppose these rules were well-enough established by tradition that everyone expected them to be enforced.”

MolochDAO

Solving collective action problems (example from whitepaper):

Say 50% of companies in the S&P500 need some public open-source accounting infrastructure. Having this infrastructure would increase each company's stock 1%. But, for any one of them to build it, it would cost then 5% of stock price.

If each company was to pay 0.01% of stock price, they could build the accounting infrastructure and benefit

MolochDAO

Guild Bank contract pools user funds

Users need to contribute funds to join, and gets voting power proportional to contribution

Membership requires a vote of current members

MolochDAO

Ragequitting

After a vote is passed, there is grace period where users that voted against can withdraw stake in Moloch

Prevents collusion - Say 99% want to pass proposal to dilute 1% down to 0. 1% can ragequit

MolochDAO

~80 members with over 6000 ETH (~$1 million) in the Guild Bank

LAOs?

Limited Liability Autonomous Organization

Developed by OpenLaw

Legally compliant DAO

Standard DAO members may be individually liable for activity of organization

Ideas on Voting

Problem with Weighted Voting

There are 3 voters, Alice, Bob, and Charlie. Alice has 100 votes, Bob has 100 votes, Charlie has 1 vote. We need at least half the total votes for the bill to pass.

I have 4 voters, Alice, Bob, Charlie, and David. Alice, Bob, and Charlie each have 100 votes. David has 1 vote. We need at least half the total votes for the bill to pass.

What are the possible outcomes in each situation?

Banzhaf Power Index

We have a set of n voters $V = \{v_1, v_2, ..., v_n\}$

We define the function $w : V \mapsto \mathbb{Z}^+$ where $w(v_i)$ is the voting weight of voter v_i

A coalition C is a subset of V representing the set of voters who vote yes.

A vote passes if

$$\sum_{v \in C} w(v) > q$$

where q is the voting threshold

Quadratic Voting

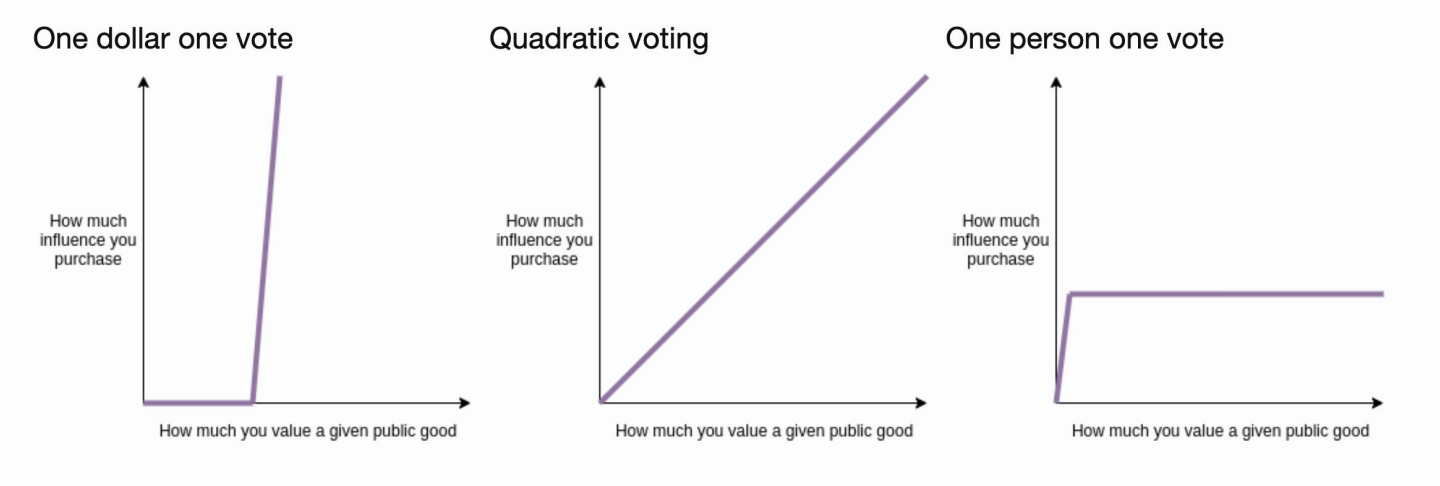
Blockchain systems often use ownership of tokens to determine voting weight

But token ownership is distributed as a power law

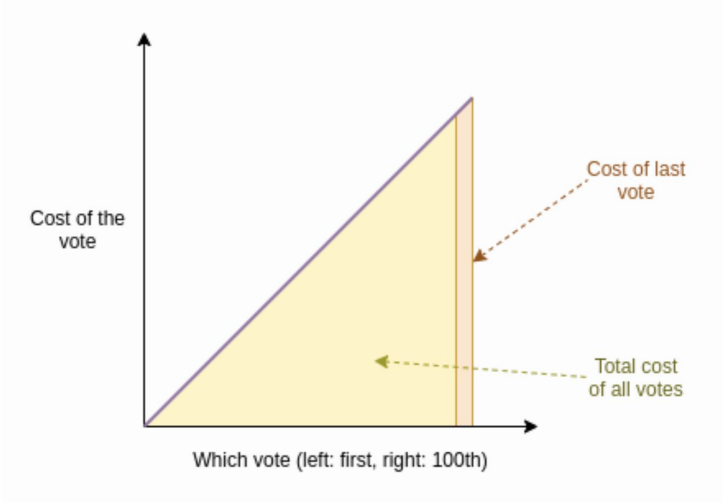
Would it be fair to vote purely by token ownership? What if one person one vote?

- One person one vote is hard on blockchains because of identity

Voting Systems



Quadratic Voting



There are some number of open proposals

Each person gets allocated some number of points

For a single proposal, to cast 1 vote, we spend 1 point. To cast 2 votes, we spend 4 points, 3 votes 9 points, etc.