

Decentralizing Decentralization

Victoria Li @Lickyvi

Disclaimer

These ideas are not necessarily mine, nor do I necessarily endorse them, but they are the result of discussions with various organizations and individuals.

I am just a teacher.

What is decentralization?

Lack of centralized whatever

i.e. No single point of failure

“

Politically decentralized: no one controls it

Architecturally decentralized: no infrastructural central point of failure

Logically decentralized: no one commonly agreed state and the system doesn't behave like a single computer

”

<https://opolis.co/off-white-paper/>

DAOs

i.e. Decentralized funding and decision-making

“

A decentralized autonomous organization (DAO)...is an organization represented by rules encoded as a computer program that is transparent, controlled by shareholders and not influenced by a central government.

A DAO's financial transaction record and program rules are maintained on a blockchain.

”

<https://opolis.co/off-white-paper/>

Bitcoin

Open Source

Anyone can view, PR, fork projects

Decentralized

Decisions are made by distributed consensus

Anyone can *propose* BIPs:

<https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md#decision-making-process>

Anyone can *make* soft forks, hard forks. Everyone *chooses* for themselves which to use.

9/2010 1MB block size soft fork
8/2017 Bitcoin Cash hard fork

<https://bitcoin.org/bitcoin.pdf>

The Dao that is spoken is not the true Dao.
The name that is named is not the true name.



張路 - http://tech2.npm.gov.tw/cheschool/zh-tw/index.aspx?content=e_1_58, Public Domain, <https://commons.wikimedia.org/w/index.php?curid=9846913>

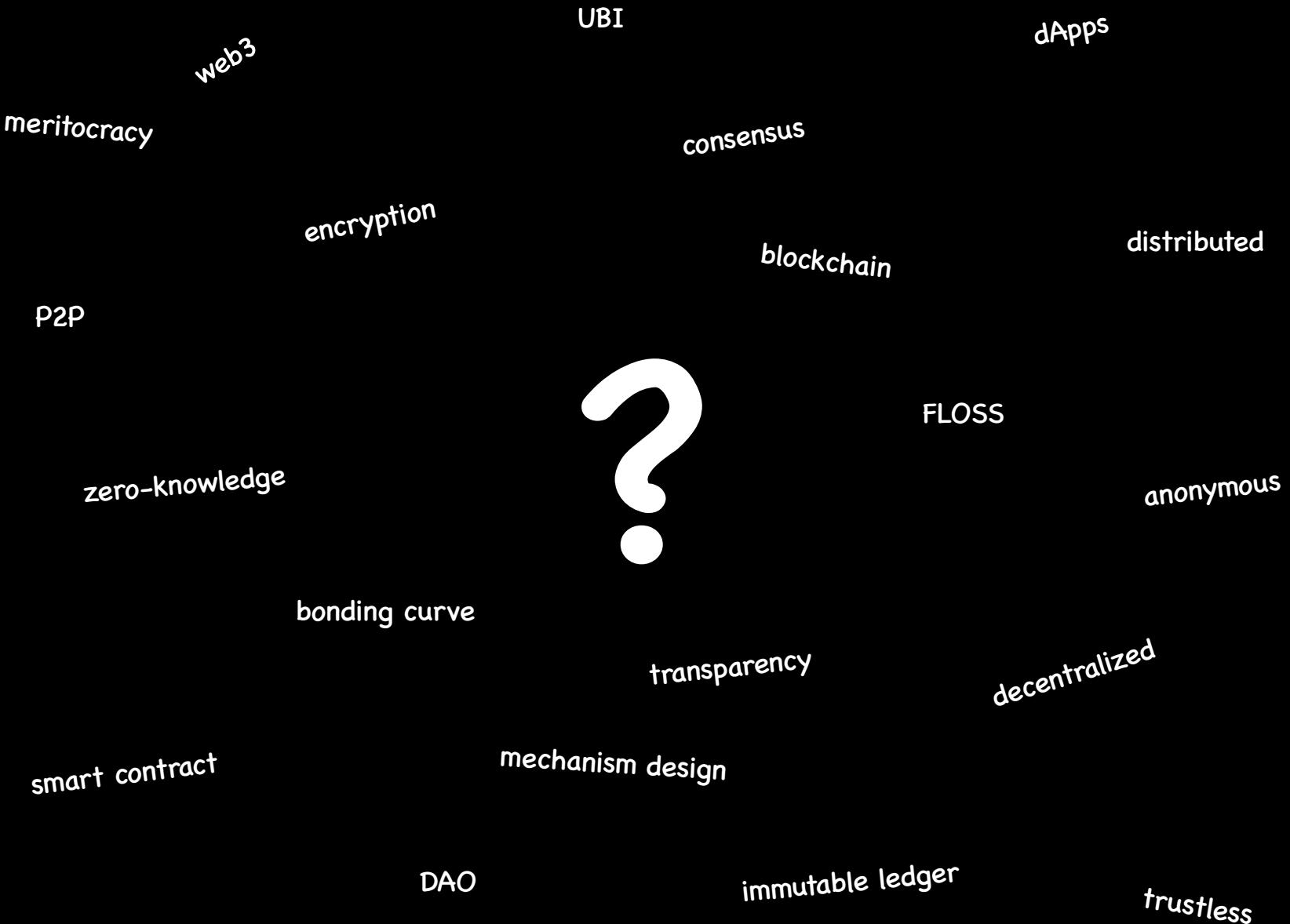
Token Engineering



<https://allthingsliberty.com/2018/09/who-picked-the-committees-at-the-constitutional-convention/>



<http://osxdaily.com/2014/02/18/still-running-old-os-x-upgrade-to-mavericks/>



Voting

Gibbard's Theorem

“Every deterministic voting scheme with at least three outcomes is either dictatorial or manipulable.”

<https://www.eecs.harvard.edu/cs286r/courses/fall11/papers/Gibbard73.pdf>

2-Outcome Vote

Doesn't exist.

Proof:

There is always an additional choice, none of the above (or all of the above).

<https://hackmd.io/@themathematicianisin/SyLhKHCWS>

Approval Voting

- 1 vote per candidate you approve of
- Approve as many candidates as you like

Manipulable: depending what you know about the current votes, you might benefit by voting differently

	1 st choice	2 nd choice	3 rd choice	
Current votes	1	1	1	→ 100
	1	4	4	→ 110

<https://www.electionsience.org/library/approval-voting/>

Quadratic Voting

“Individuals pay for as many votes as they wish using a number of ‘voice credits’ quadratic in the votes they buy.”

<https://ssrn.com/abstract=2003531>

Futarchy/Signaling Markets

“Vote on Values, Bet on Beliefs”

- 1. Trade “I pay you \$1 if V wins” assets (V assets)
- 2. price = $E[\text{pay}] = P(V \text{ wins})$
- 1. Vote on welfare = $W \in [0,1]$ measurement method
- 2. Trade “I pay you $\$W/(\text{current price of B assets})$ if B wins” assets
- 3. Calculate W
- 4. price = $E[\text{pay}] = P(B)E[W|B]/P(B) = E[W|B]$

“When speculative markets clearly estimate that a proposed policy would increase national welfare, that policy becomes law.”

<http://hanson.gmu.edu/futarchy2013.pdf>

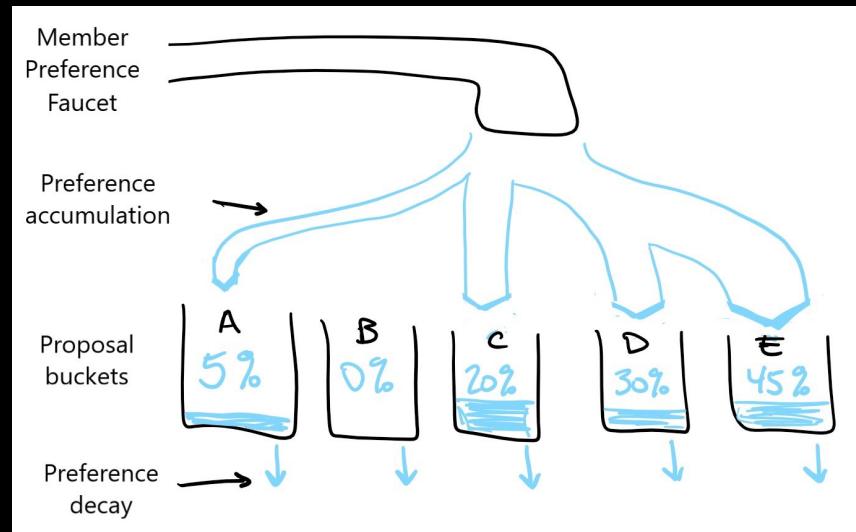
Continuous Voting

Voting by Contributing

- Basically, do what you want, but bear the consequences
- Create whatever projects you want, support whatever projects you want
- What if projects conflict?

See Ownership

Conviction Voting



- In progress as of 8/24/2019

See Merit Signaling

<https://medium.com/giveth/conviction-voting-a-novel-continuous-decision-making-alternative-to-governance-aa746cfb9475>

<https://github.com/disclosure-exchange/whitepaper/wiki/R&D#voting-by-contributing>

Experiments

Quadratic Voting - CO House Dem Caucus 2019

In a modified version of quadratic voting, Colorado legislators each got 100 virtual tokens to buy votes on a number of measures. "There was a pretty clear signal on which items, which bills, were the most important for the caucus to fund," says one state rep.

 JOE AMON/THE DENVER POST/GETTY IMAGES



<https://www.wired.com/story/colorado-quadratic-voting-experiment/>

Signaling Markets - Augur



https://www.reddit.com/r/mkrgov/comments/bcfx9x/executive_vote_raise_the_stability_fee_by_4_to_a/

Continuous Approval Voting (by MKR holders) - MakerDAO

16 ↓ | 🗳 [Executive Vote] Raise the Stability fee by 4% to a total of 11.5% per year

In February, the Stability Fee was increased twice, each time by 0.5%. In March, the Fee was raised by an additional 2%, and then by 4% two weeks later. The impact of these combined increases was insufficient to restore the peg, indicating that the appropriate rate is still higher.

https://www.reddit.com/r/mkrgov/comments/bcfx9x/executive_vote_raise_the_stability_fee_by_4_to_a/

Plutocracy - AGP42

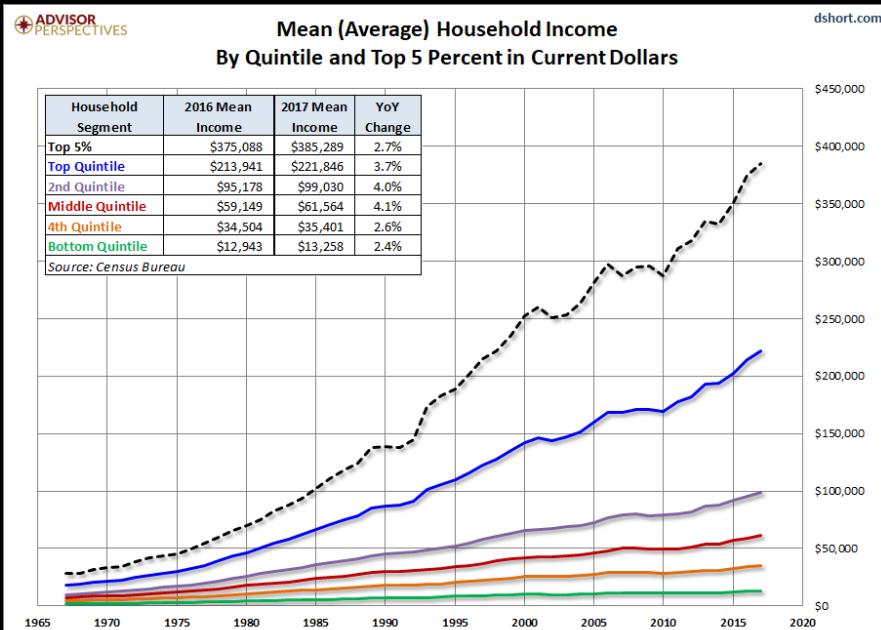
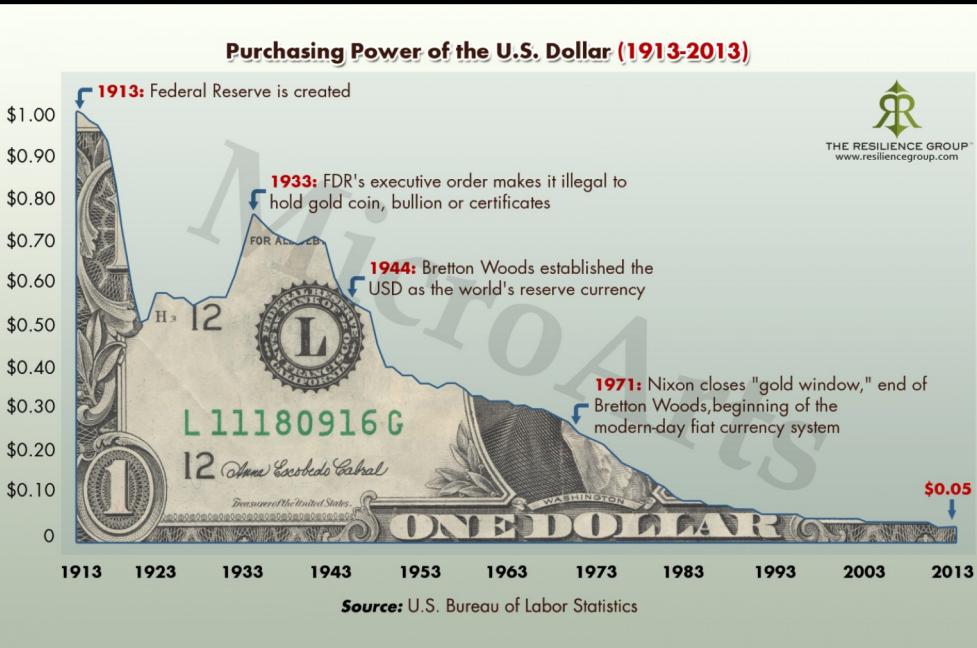


<https://www.evanvanness.com/post/184616403861/ragon-vote-shows-the-perils-of-onchain-governance>

Cryptoeconomics

On Inflation goods/\$

\$/goods



Inflation Funding – EIP2025

 **James Hancock**
@JHancock

Replying to @JHancock

EIP 2025 is withdrawn. I reverted the changes to the original proposal for historic purposes as that has been the version that most was discussed.

4 05:11 · 27 Jul 2019 · Toronto, Ontario

<https://www.cryptoglobe.com/latest/2019/08/circle-research-examines-the-debate-around-ethereums-funding-model/>

On Sustainability

Transparency

1. Decentralized
2. Trustless
3. Peer-to-Peer (no middle-men)

Meritocracy

- Meritocracies maximize merit
- Nature maximizes efficiency
- How do we achieve both?

<https://hackernoon.com/the-history-of-money-the-future-of-bitcoin-and-the-cryptocurrency-economy-5cc25e808275>

<https://hackmd.io/@themathematicianisin/SyLhKHCWS>

Funding

Augmented Token Bonding Curves

A continuous, self-sustaining, fully-backed, native currency:

$R(C)$ = token bonding curve

R = funds in reserve

C = tokens in circulation

Purchase price determined by reserve funds: $P(R) = dR/dC$

Redemption value backed by reserve funds: $S(R)=R/C(R)$

Proved: $R < C(R)dR/dC$ so $R=aC^k$ for $k > 1$, $a = 1/V_0$

Value increases as Reserve funds increase

https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf

<https://medium.com/giveth/deep-dive-augmented-bonding-curves-3f1f7c1fa751>

<https://hackmd.io/@themathematicianisin/BkikbN2kr>

Investment Model

Anyone contributes at any time:

1. Reserve Fund by purchasing tokens
2. Project Fund via $1-\lambda\%$ transaction or service fee
3. Work on projects

Contributors are rewarded respectively by:

1. Tokens whose value is tied to a good/service
2. Development of said good/service
3. Paid by Resource Allocation

Transaction fee is determined by the market (Merit Signaling)

Tokens are used as Currency:

- A. Store of Value - redeemed for the underlying asset
- B. Medium of Exchange - exchanged for other tokens
- C. Unit of Accounting - purchase goods/services

<https://github.com/disclosure-exchange/whitepaper/wiki/R&D#funding>

Resource Allocation

Mechanism Design

	Progressive Auction	Dutch Auction
Mechanism	Increase price to last bid	Decrease price to 1st bid
Homogeneous		Lower variance
Non homogeneous		Manipulable Not always Pareto-optimal
Both	$E[\text{price}] = 2^{\text{nd}}$ highest bid Pareto-optimal	$E[\text{price}] = 2^{\text{nd}}$ highest bid

Sealed-bid auction to highest bidder at 2nd highest price achieves optimal resource allocation

<https://www.cs.columbia.edu/coms6998-3/lecture1-auctions.pdf>

<https://hackmd.io/@themathematicianisin/Sk-hh3Zqr>

Merit Signaling

For each project:

Step 1

Contributors continuously use their tokens to signal % conviction (merit) of subprojects

Step 2

This equals the % of incoming project funds received by the subprojects

Apply recursively to subprojects/.../tasks/subtasks/contributors.

<https://github.com/disclosure-exchange/whitepaper/wiki/R&D#meritocracy>

Ownership

REMEMBER WHEN WE PROSECUTED MICROSOFT
FOR BUNDLING A BROWSER WITH AN OS?

IMAGINE THE FUTURE WE'D LIVE IN IF
WE'D BEEN WILLING TO LET ONE TECH
COMPANY AMASS THAT MUCH POWER.

THANK GOD WE
NIPPED THAT
IN THE BUD.



https://www.explainxkcd.com/wiki/index.php/1118:_Microsoft



<http://blogs.reuters.com/photographers-blog/2012/11/26/house-in-the-middle-of-the-road/>

Harberger Taxes

Owner <--> Pay Tax

“Even if the revenue from such taxes are completely ignored, the cost of keeping works proprietary as opposed to releasing them open source would incent users of the license to include their derivative works in the commons rather than keeping the work proprietary.”

<https://medium.com/hive-commons/harberger-taxation-and-open-source-58dcbab140d>

Ownership <--> Competence

“Investors (through token bonding curve) fund competence of the team building the product, not the product itself. This will take us to the Future of Ideas.“



<https://hackmd.io/@themathematicianisin/SyLhKHCWS>

https://en.wikipedia.org/wiki/Gate_Tower_Building

In Summary

Decentralization and DAOs:

- Voting
- Funding
- Resource Allocation
- Ownership

A Long Long List

Too many people to fit here, so...

Thank You Everyone!

- Bitcoin Training Conference (C4)
- Opolis
- AragonProject
- Giveth
- Native
- Council for the Advancement of Blockchain Technology Use
- Securities and Exchange Commission
- Disclosure Exchange
- Colorado Blockchain (Various meetups)
- You