KAIST
School of Computing

Web3@KAIST

Building Web3 Apps to Solve Real Problems

Building Web3 & Blockchain Applications
(CS492 Special Topics in Computer Science)
Spring 2023

Centralized Decentralization
Simple Economics of DPoS Governance

Guest Lecture 13 (2023-04-26)

Guest Speaker

Seungwon (Eugene) Jeong

Assistant Professor

Metanomics Lab, BTM KAIST

http://web3classdao.xyz/kaist/

Outline

1. DPoS (Delegated Proof-of-Stake)
   - NPoS, LPoS
2. Centralized Decentralization
   - Tron Foundation's Steemit acquisition
   - Theoretical foundation for DPoS voting
   - DPoS Governance Attack Game
   - Does VPA (votes per account) matter?
   - Optimal VPA: minimizes takeover risk, maximizes voting flexiblity

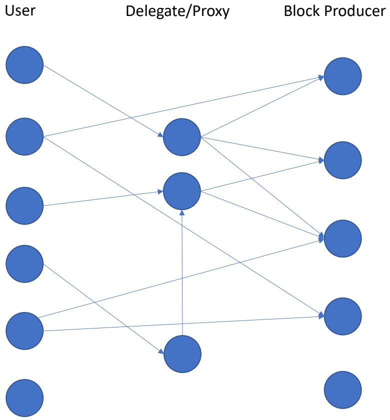
DPoS (Delegated Proof-of-Stake)

DPoS (Delegated Proof-of-Stake)

Disclaimer: This talk is not about which consensus mechanism is better.

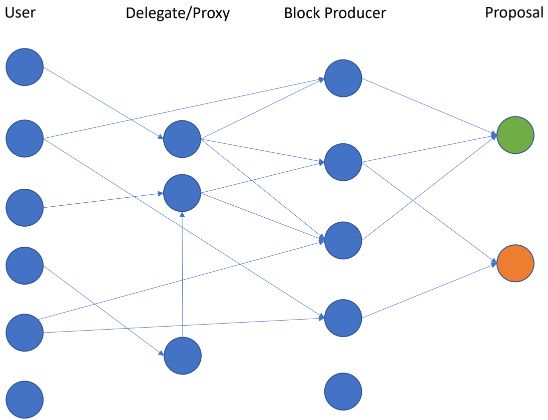
- Invented by Daniel Larimer (2014), and first applied to BitShares.
- Adopted by EOS, Steem/Hive, Tron, Lisk, Ark, etc.
- Block producers (BPs, also called witnesses, or validator) verify the transactions, produce a new block, and then get a reward.
- BPs are elected through votes by users (accounts), which is weighted by their stakes of the token.
- Users can directly vote for BP, or indirectly vote via delegates (proxy).
  - "Delegated" in DPoS does not mean proxy only. It refers to both *direct* (vote for BP) and *indirect* voting (vote for proxy).
  - "Delegated" in the sense that a normal user does not produce a block or make a decision directly. BP does the job via the delegation of power.

DPoS: BP election



- A user is an account.
- Essentially, delegates and BPs are also users.
- A delegate (proxy) is a user who receives delegation.
- A BP is a user who receives enough number of votes to be a BP.

DPoS: fork election



- For each proposal (e.g., fork), each BP approves or disapproves it.
- The proposal is approved if supermajority of BPs approves it.

Examples of DPoS blockchains

Table: **DPoS blockchains**

	BP (n)	BP for fork (k)	VPA (v)
Steem	20	17	30
Tron	27	19	1
EOS	21	15	30
Lisk	101	68	101

- BP (n): number of BPs
- BP for fork (k): number of BPs needed for a fork (or any on-chain decision)
- VPA (v): number of votes allowed per account

- Based on stake-weighted votes, n topmost users are elected as BPs.
- Any on-chain proposal (e.g., fork) is approved if at least k out of n BPs agree.
- Previously, VPA had been chosen without any theoretical foundation.

Advantages of DPoS

- energy efficient
  - BPs are trusted, so no additional work is needed, as opposed to the *Proof-of-Work* (PoW) consensus.
- faster and more scalable
- more democratic?
  - similarity between the blockchain election and the real-world election.

Disadvantages of DPoS

- centralization
  - Some poeple say "DPoS is largely considered to be the most decentralized approach to consensus mechanism." But in reality?
  - One reason: VPA had been chosen without any theoretical foundation.
    - e.g., in a Lisk proposal,

Forum member "Consensus" suggested lowering this number to 20. This would limit the ability to share votes in a coalition and would improve decentralization of the network. On the other hand, "cc001" would prefer to increase it to 131.

- vote buying
- less secure (in the sense that the number of BPs are normally small)

NPoS, LPoS

NPoS (Nominated PoS)

- As opposed to DPoS, nominators are subject to loss of stake if they nominate a bad validator.
- Polkadot, Kusama

LPoS (Liquid PoS)

- Two types of validators (baker and endorser)
  - baker: create blocks
  - endorser: agree on blocks
- As opposed to DPoS (in terms of technical requirements), any user can become a validator (if he has enough coins).
- Tezos

LPoS vs DPoS

	Liquid-proof-of-stake	Delegated-proof-of-stake
Delegation (Purpose)	Optional (minimizes dilution of small token holders).	Required to elect block producers (enables greater scalability.
Barrier to Entry	6000ꜩ, modest computing power and reliable internet connection.	Professionalized operations with significant computing infrastructure. Competition from other delegates.
Validator Set	Dynamic (size not fixed), limited by total supply of tez.	Fixed size. Between 21 (EOS) and 101 (Lisk).
Design Priorities	Decentralization, accountable governance, and security	Scalability and usable consumer applications

`https://opentezos.com/tezos-basics/liquid-proof-of-stake/`

Centralized Decentralization

Bitcoin Genesis Block

CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f7

(decoded) ┘��↔┌┘EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks


THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

99p

Decentralization

- *Decentralization* is often claimed as one of the virtues of blockchain.
- One important aspect of decentralization is *governance*.
- That is, a blockchain should not be controlled by a centralized entity.
- Thus, not using founders' stake for voting is normally expected.

Tron Foundation's Steemit acquisition

Disclaimer: This talk is not about who's right and who's wrong.

- The Steem blockchain that has the main DApp, Steemit (`https://steemit.com`), a social media platform.
- In February 2020, the Tron Foundation acquired Steemit Inc that mainly developed and maintained the Steem blockchain.
- Previously, Steemit Inc promised not to use their stake for voting.
- However, the Tron Foundation did not mention such an agreement during the acquisition.
- Most top incumbent BPs covertly implemented and executed a reversible fork (ver 0.22.2) that prohibits a pile of tokens (previously owned by Steemit Inc) from voting and transferring, expecting that they could get a similar agreement from the Tron Foundation.

Tit-for-Tat Governance Attacks

- After fork 0.22.2, the Tron founder promised (on a blog post) not to use his vote, but after a few days, he created 20 ($n = 20$ for Steem) new accounts and voted for them using his stake and changed all of the top 20 BPs by his single account.
- To help the Tron Foundation, some cryptocurrency exchanges also participated in the vote via delegation even using *custodial tokens* (i.e., customers' tokens), but they retracted their votes later and apologized.
- The new top 20 BPs executed a tit-for-tat fork that seized the tokens of some previous top BPs.

There's no better way to put this: One man's "hack" is another's "legitimate exercise of power by a blockchain's duly elected leaders."[1]

[1] See `https://www.coindesk.com/steem-community-mobilizes-popular-vote-in-battle-with-justin-sun`, link to "Steem Community Mobilizes Popular Vote in Battle With Justin Sun."

DPoS as an indirect election

In terms of voting theory, DPoS is an *indirect* election.

- (BP election) first election uses a multiwinner voting rule based on approval preferences with a cap on ballot size
- (fork election) second election uses a supermajority voting rule.

An election based on weighted approval preferences is $E = (N, M, A, \overline{b}, w)$

- $N = \{1, 2, ..., \overline{n}\}$ is the set of *voters*
- $M = \{c_1, c_2, ..., c_{\overline{m}}\}$ is the set of *candidates*
- A is an *approval-based voting profile* with a *cap of ballot size* $\overline{b}$, i.e., a function $A : M \to 2^M$ such that $|A(i)| \leq \overline{b}$
- w is a *weight profile*, i.e., a function $w : N \to \mathbb{R}_+ \equiv \{x \in \mathbb{R} : x \geq 0\}$.

That is, $A(i)$ is the set of candidates that voter i finds acceptable, and $w(i)$ is the weight of voter i.

A multiwinner election rule based on weighted approval preferences is a function R such that

- $R(E, m) \in S_m(M) \equiv \{S \subseteq M : |S| = m\}$ is a size-m subset of candidates that receives the highest sum of the scores from voters
- the score that a candidate c gets from a voter i is $\mathbb{1}(c \in A(i)) \cdot w(i)$.

DPoS elections: BP election and fork election

- n: number of BPs
- k: number of BPs for fork
- v: VPA (votes allowed per account)

- Accounts vote for up to v *block producers* (BP) among accounts themselves.
- A vote is weighted by the amount of tokens that each account holds.
- There is no discount on voting for multiple candidates.
- n elected (i.e., n topmost in terms of weighted votes) BPs vote for a *fork* decision (i.e., a change of the rule of the blockchain) by a supermajority voting rule such that the decision is approved if at least k out of n BPs agree.

DPoS Governance Attack Game

We consider the DPoS Governance Attack Game, or simply the Governance Game.

1. In the first stage, Defender (with fixed δ tokens) votes for BPs.
2. In the second stage, Attacker acquires α tokens at a unit cost p and votes for BPs, where $p\alpha < 1$.

- Based on the rankings of the total weighted vote count, n BPs are elected (with a tie-breaking in favor of Attacker for simplicity).
- The payoffs of Attacker and Defender, denoted by π_A and π_D, are defined as follows:

$$\pi_A = \mathbb{1}(|BP_A| \geq k) - p\alpha$$
$$\pi_D = \mathbb{1}(|BP_A| < k) + p\alpha$$

Even distribution

Proposition (Even distribution)

In the governance game,

1. Attacker's voting for k candidates with equal shares, and
2. Defender's voting for $n-k+1$ candidates with equal shares and Attacker's voting for k candidates with equal shares is an equilibrium path of play in a subgame-perfect Nash equilibrium, which is unique when $v \leq \min\{k, n-k+1\}$.

Does VPA matter?

Whether VPA affects the minimum stake that Attacker should acquire for takeover (i.e., whether α^* is independent of v), may not still be clear.

Q. α^* (the minimum stake that Attacker should purchase for takeover) is

1. increasing in v (i.e., α^* decreases as v decreases)
2. decreasing in v (i.e., α^* increases as v decreases)
3. constant
4. none of the above

It may be nontrivial because

- intuitively, decreasing v may decrease the "power" of one account
- but this applies to all accounts

Does VPA matter?

Example

Suppose $n = 3$ and $k = 2$, i.e., if at least 2 out of 3 BPs agree, they can take over the blockchain, and Defender has $\delta = 100$ tokens. We consider three values of VPA v to find $\alpha^*(n, k, v, \delta)$.
(i) $v = 3$: Defender should vote for all three (or at least 2) candidates with equal shares of 100. Since Attacker can vote for up to 3 candidates, in order to have 2 BPs elected, Attacker only needs 100 tokens, i.e., $\alpha^*(3, 2, 3, 100) = 100$.
(ii) $v = 2$: Defender should vote for 2 candidates with equal shares of 100. Since Attacker can vote for up to 2 candidates, in order to have 2 BPs elected, Attacker still only needs 100 tokens for the takeover, i.e., $\alpha^*(3, 2, 2, 100) = 100$.
(iii) $v = 1$: Defender should vote for 2 candidates with equal shares of 50, i.e., by dividing 100 tokens into 2 accounts. Since Attacker can also vote for only one candidate per account, in order to have 2 BPs elected, $\alpha^*(3, 2, 1, 100) = 2 \times 50 = 100$.
Moreover, one can easily check that $\alpha^*(3, 2, v, \delta) = \delta$ for all $v \geq 1$.

Does VPA matter?

- $\alpha^*(n, k, v, \delta)$ is independent of v, in general?
- No (in general).
- Interestingly, α^* can be either increasing or decreasing in v, depending on the combination of n and k.
- If the majority of BPs is needed for a fork, a smaller VPA requires a larger stake for takeover, but only up to a certain point.
  - That is, a so-called "one vote per account" rule may not be needed.

TRC (takeover resistance coefficient)

The takeover resistance coefficient (TRC), denoted by $\tau(n, k, v)$, is the minimum ratio of Attacker's stake to Defender's stake for takeover.

Theorem (TRC)

In the governance game, the minimum stake required for Attacker to take over the governance is,

$$\alpha^*(n, k, v, \delta) = \tau(n, k, v) \cdot \delta, \tag{1}$$

where

$$\tau(n, k, v) = \frac{\max\{k, v\}}{\max\{n - k + 1, v\}}. \tag{2}$$

Monotonicity of TRC

Corollary

The takeover resistance coefficient $\tau(n,k,v)$ is monotone in v, and the monotonicity depends on the combination of n and k as follows:

1. *If $k > \frac{n+1}{2}$, then $\tau(n,k,v)$ is decreasing in v, and*

$$\tau(n,k,v) = \begin{cases} \frac{k}{n-k+1} & v \leq n-k+1, \\ \frac{k}{v} & n-k+1 \leq v \leq k, \\ 1 & v \geq k. \end{cases}$$

2. *If $k = \frac{n+1}{2}$, then $\tau(n,k,v) = 1$.*
3. *If $k < \frac{n+1}{2}$, then $\tau(n,k,v)$ is increasing in v, and*

$$\tau(n,k,v) = \begin{cases} \frac{k}{n-k+1} & v \leq k, \\ \frac{v}{n-k+1} & k \leq v \leq n-k+1, \\ 1 & v \geq n-k+1. \end{cases}$$

TRC of DPoS blockchains

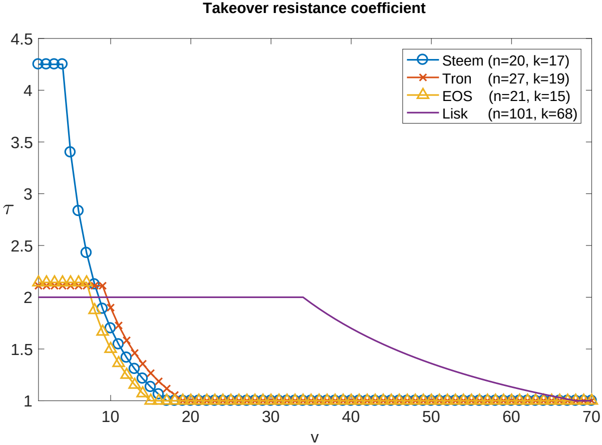


Figure: The takeover resistance coefficient (TRC), denoted by $\tau(n, k, v)$, is the minimum ratio of Attacker's stake to Defender's stake for takeover. The figure shows the TRCs with their actual parameters of n (number of BPs) and k (number of BPs for fork), varying VPA v.

Policy Implication

Table: **DPoS blockchains**

	BP (n)	BP for fork (k)	VPA (v)	**optimal VPA** (v^*)
Steem	20	17	30	4
Tron	27	19	1	9
EOS	21	15	30	7
Lisk	101	68	101	34

- BP (n): number of BPs
- BP for fork (k): number of BPs needed for a fork (or any on-chain decision)
- VPA (v): number of votes allowed per account
- optimal VPA (v^*): the maximum VPA that has the maximum TRC

- v^* minimizes the takeover risk, while maximizing voting flexiblity.
- "one vote per account" is not needed (unnecessary account creations may occur.)

Maximum TRC depending on *k*

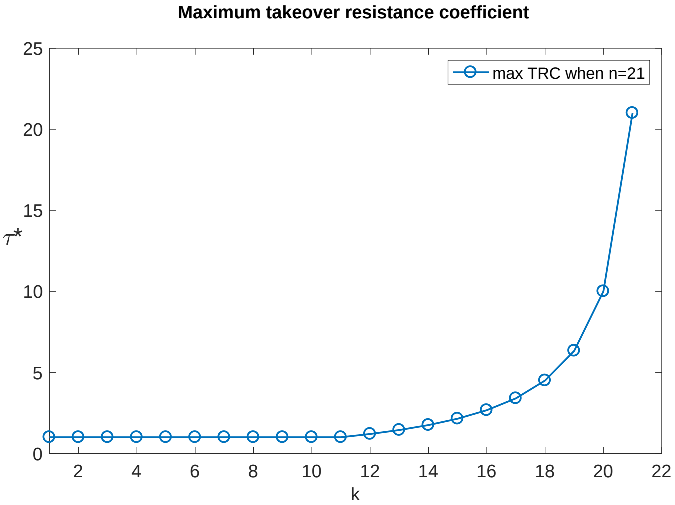


Figure: **Maximum takeover resistance coefficient.** The figure shows the maximum takeover resistance coefficient $\tau^* = \tau^*(n, k) = k/(n-k+1)$. For a fixed n (number of BPs, $n = 21$ in this figure), the marginal increase of TRC τ^* increases as k (number of BPs for fork) increases.

Conclusion

- DPoS blockchains may be prone to centralization.
- The "optimal" VPA can be chosen with a microeconomic foundation.
  - minimizes the takeover risk, while maximizing voting flexiblity.
- "One vote per account" is not needed.
  - less flexible, so unnecessary account creations may occur.
- Which (n, k) (or even v) should be used may ultimately depend on many factors including technical limitations and philosophies of the blockchain.