

How Hard is Takeover in DPoS Blockchains?

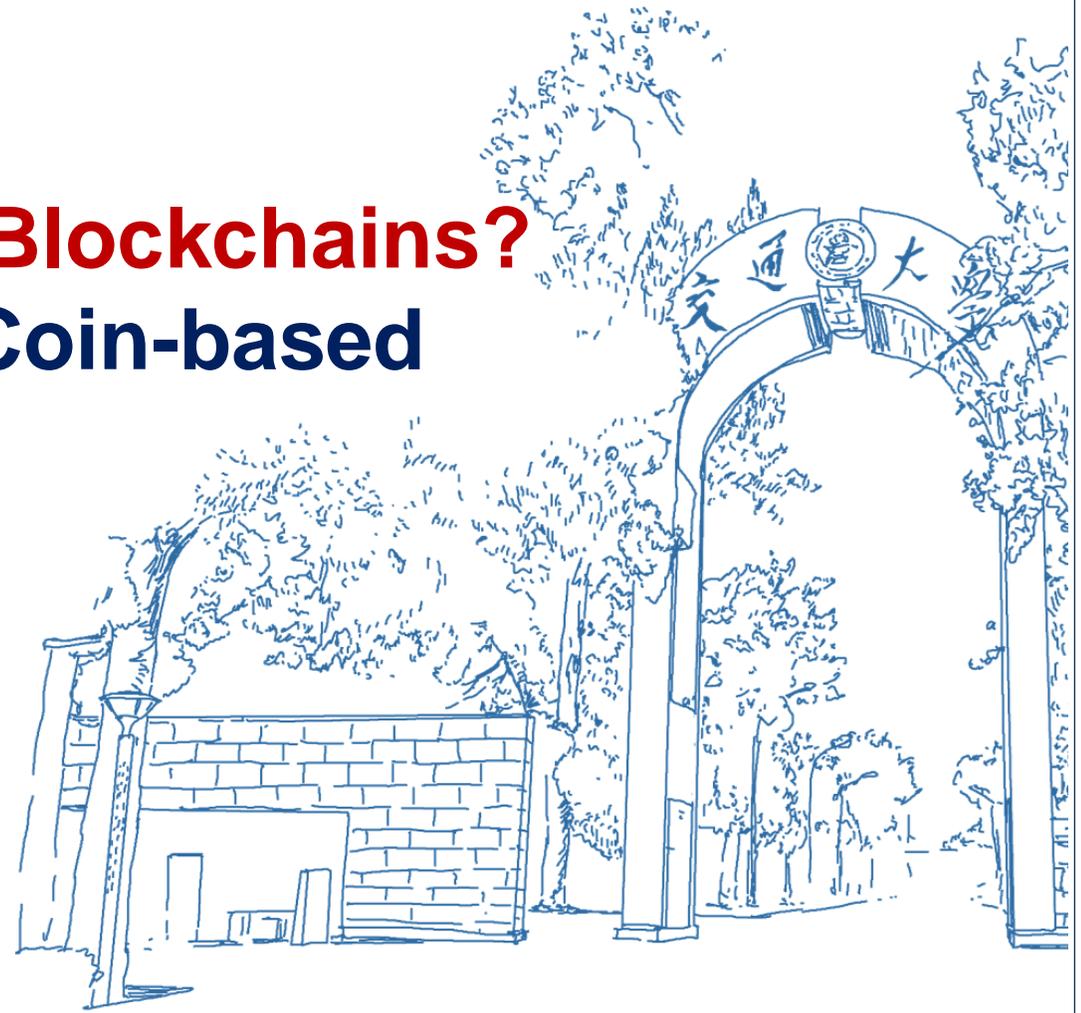
Understanding the Security of Coin-based Voting Governance

Chao Li¹, Balaji Palanisamy², Runhua Xu³,
Li Duan¹, Jiqiang Liu¹, Wei Wang¹

¹Beijing Jiaotong University

²University of Pittsburgh

³Beihang University



北京交通大学
BEIJING JIAOTONG UNIVERSITY



University of
Pittsburgh



北京航空航天大学
BEIHANG UNIVERSITY



> Outline <

01 What is Governance

02 Voting Governance

03 Hostile Takeover

04 Takeover Resistance

05 Conclusion



01

What is Governance

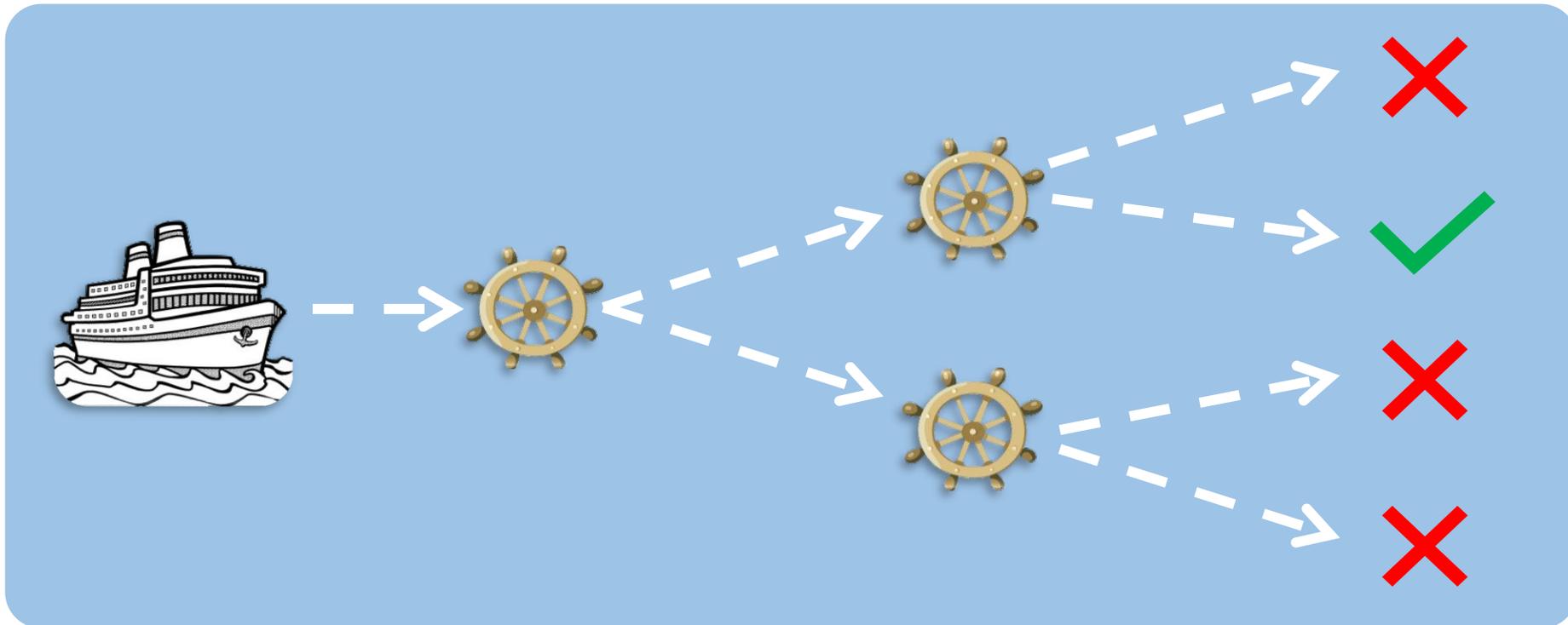
'Governance' as the Rudder



北京交通大学

BEIJING JIAOTONG UNIVERSITY

- In the vast ocean of Web 3.0, governance is like a rudder.
 - Without a captain, how can a ship navigate and plan a safe course?



Origin of 'Governance'



北京交通大学
BEIJING JIAOTONG UNIVERSITY

- The term 'governance' has a long history.
 - It originates from the Greek verb kubernaiein [kubernáo] (**meaning 'to steer or guide'**) and is thought to have first appeared in the works of Plato;
 - In early English, it was occasionally used to refer to the specific activity of **'ruling a country by an individual'**;
 - The first use of **'institutional governance'** is thought to be in the 1885 article 'The Governance of England';
 - Not until the 1990s did economists and political scientists give 'governance' a broader meaning, including **'public governance'**, **'corporate governance'**, and **'global governance'**, and it was spread by institutions such as the United Nations, International Monetary Fund, and World Bank.

Meaning of 'Governance'



北京交通大学

BEIJING JIAOTONG UNIVERSITY

Governance refers, therefore, to all processes of governing,
whether undertaken by a *government, market, or network*,
whether over a *family, tribe, formal or informal organization, or territory*,
and *whether through laws, norms, power, or language*.

The term '**governance**' draws attention to **processes of decision-making and ruling**.

source: Mark Bevir. *Governance: A very short introduction*. OUP Oxford, 2012.

'Governance' Incidents in Web 3.0



■ The DAO Incident

The first breach of 'code is law'

Vote: TheDAO Hard Fork

How to vote?

Make a 0-ETH transaction to the YES or NO address to vote respectively.

All the ETH under the from-address will be counted as corresponding ballots.

For the transactions to be done successfully, a minimum amount of transaction fee of 0.0006 ETH is required.

If your wallet (for instance, Mist) does not support 0-ETH transactions, a minimal amount (e.g. 0.0001 ETH) is recommended. The smart contract will send back any amount of ETH it receives automatically.

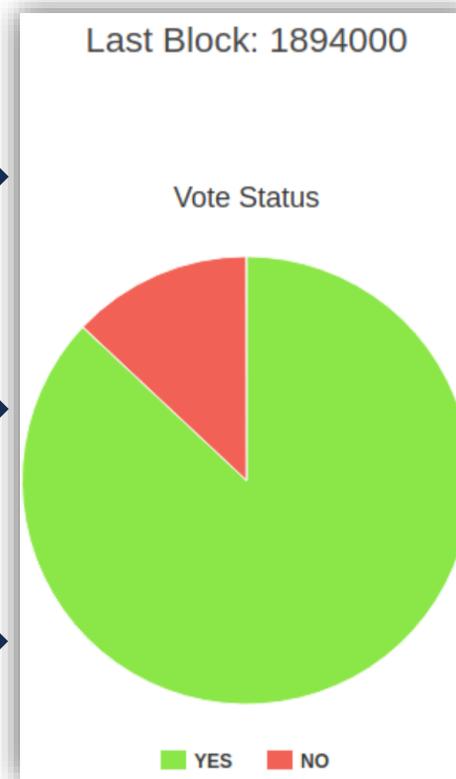
The status is an on-going real-time counting.

Vote YES: `0x3039d0a94d51c67a4f35e742b571874e53467804`

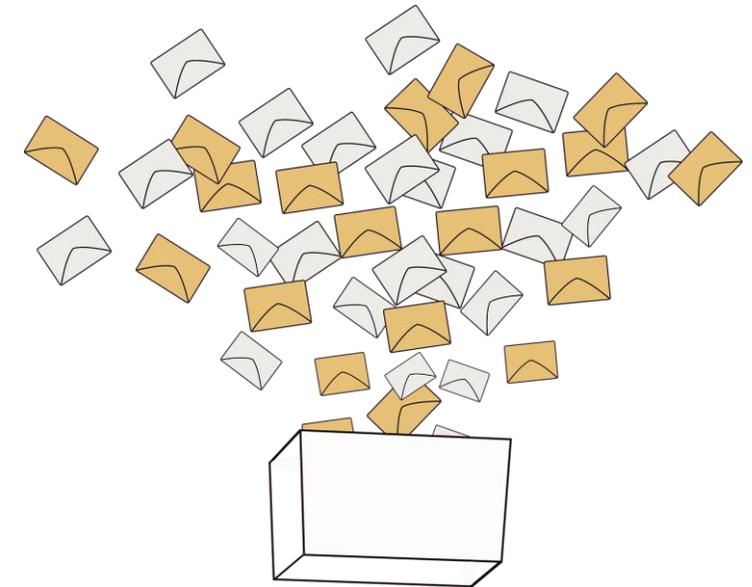
Vote NO: `0x58dd96aa829353032a21c95733ce484b949b2849`

YES

NO



Referendum



source: <http://v1.carbonvote.com/>

Image by Felipe Blasco from Pixabay

'Governance' Incidents in Web 3.0



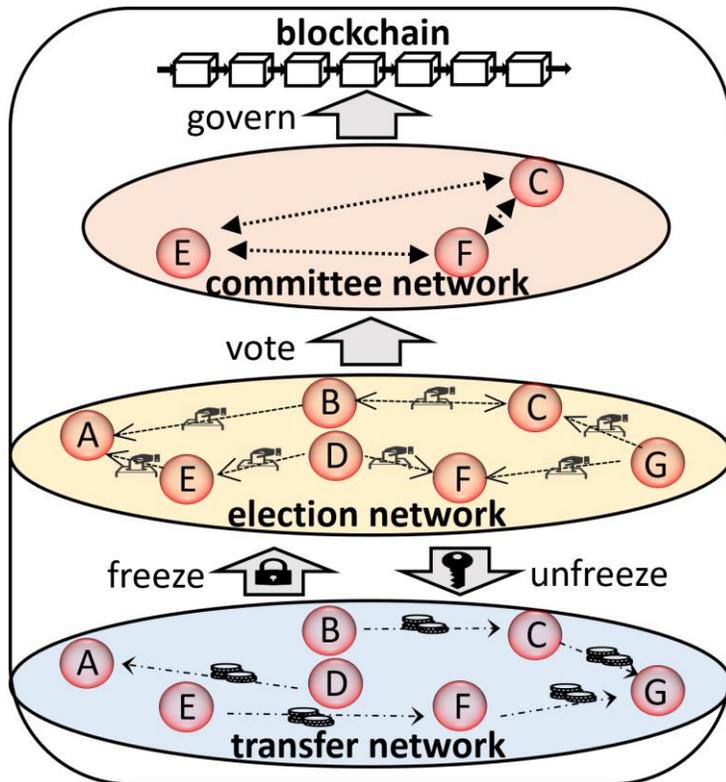
北京交通大学

BEIJING JIAOTONG UNIVERSITY

■ TRON-Steem Takeover Incident

The first *'hostile takeover'*

DPOS Consensus



Overview

Timeline

2018-01, Steem in the TOP 25 at coinmarketcap.com

2020-02-24, Steem BPs implemented the **Fork 0.22.2 to limit transactions performed by sold accounts** (e.g., @steemit)

2020-03-20, Hive hard forked Steem, airdropping HIVE coins, excluding pre-mined coins

2016-03, Steem went live

2020-02-14, TRON founder purchased Steemit Inc., including accounts holding pre-mined coins (e.g., @steemit)

2020-03-02, within one hour, **all BPs were replaced**, and new BPs immediately implemented the **Fork 0.22.5 to undo the changes of 0.22.2**



02

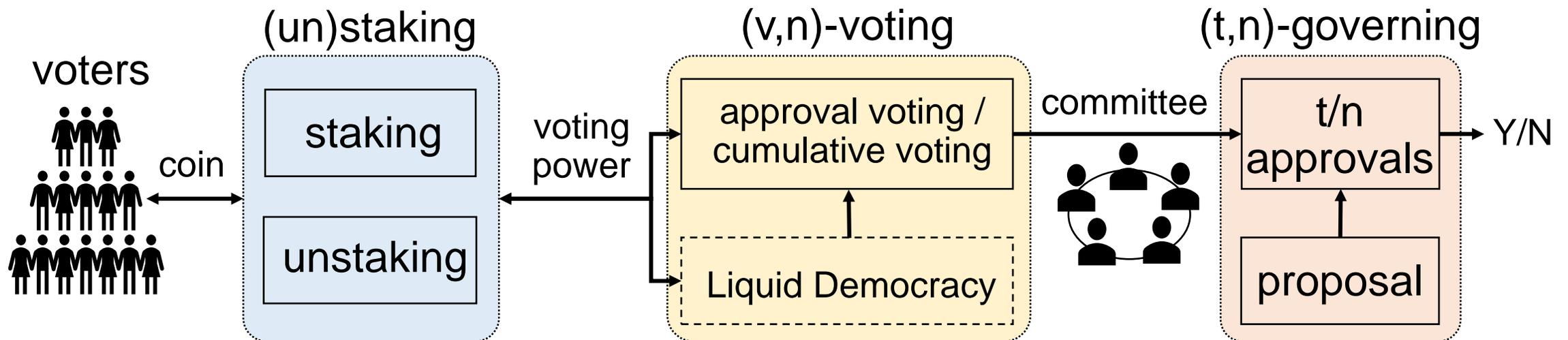
Voting Governance

Coin-based Voting Governance



■ Three Phases of Coin-based Voting Governance

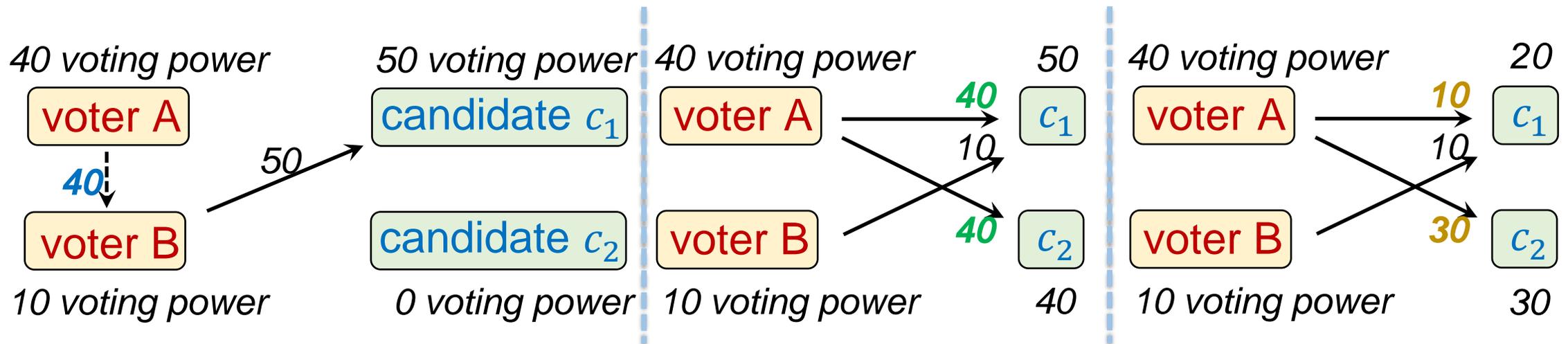
1. **Staking**: individual coins are converted into individual voting power
2. **(v,n)-voting**: individual voting power is aggregated
3. **(t,n)-governing**: pooled voting power is converted into governance decision-making power



Voting Rules



- The voting phase may employ different voting rules for aggregating individual voting power, leading to varied outcomes.
 - **Liquid Democracy**: Voting power can be **delegated** to others.
 - **Approval Voting**: Voting power is **reusable**.
 - **Cumulative Voting**: Voting power is **not reusable**.





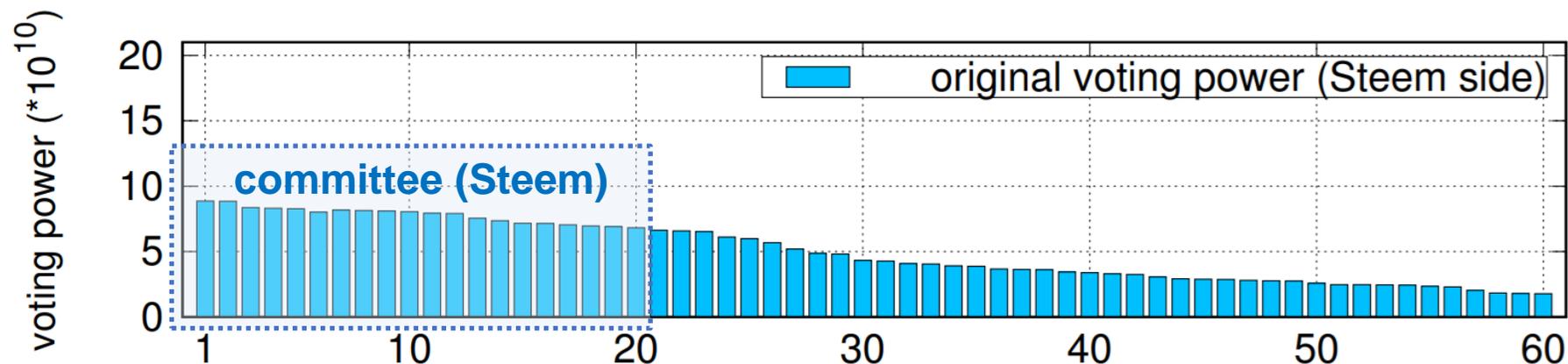
03

Hostile Takeover

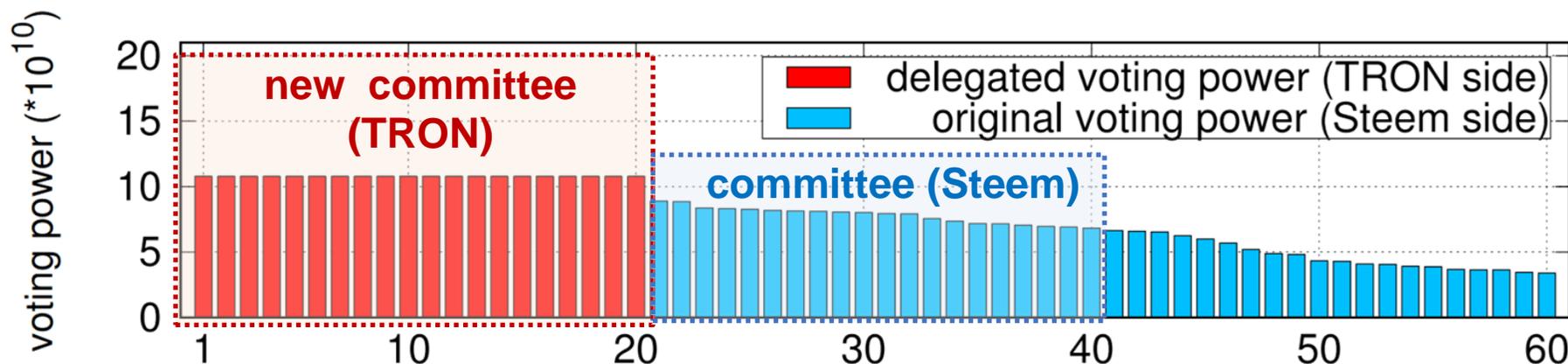


TRON's Takeover of Steem

- Before the attack, the top 20 ranked candidates in Steem formed a committee.



- Within 27 minutes, 20 candidates controlled by TRON founder took over the committee.



Steem's Resistance Against Takeover



CALL TO ACTION! EARN UPVOTES TO VOTE FOR WITNESSES

 theycallmedan (75) · 在 #steem · 3年前 (edited)

The world will remember that free people stood against a tyrant, that hodlers stood against exchanges and before this battle is over that even Tron can bleed.

We have struck a telling blow in this war for STEEM! @yabapmatt is now our #1 and we only need 4 to foil their takeover attempt.

Witness Voting
You have 1 vote remaining. You can vote for a maximum of 30 witnesses.

| Witness | Information |
|------------------|----------------|
| 01 yabapmatt | witness thread |
| 02 goodguy24 | external site |
| 03 nicety001 | external site |
| 04 tuku2049 | external site |
| 05 happyHu123 | external site |
| 06 age110000 | external site |
| 07 bostonawesome | external site |
| 08 jumphigh | external site |
| 09 hunger365 | external site |
| 10 waitoryou1 | external site |
| 11 onestopaday | external site |
| 12 car2001 | external site |
| 13 aheadofblow | external site |

THIS IS THE 4TH QUARTER STEEMIANS! CHIN STRAPS ON!

Prove your votes below to earn a nice sized upvote from me!

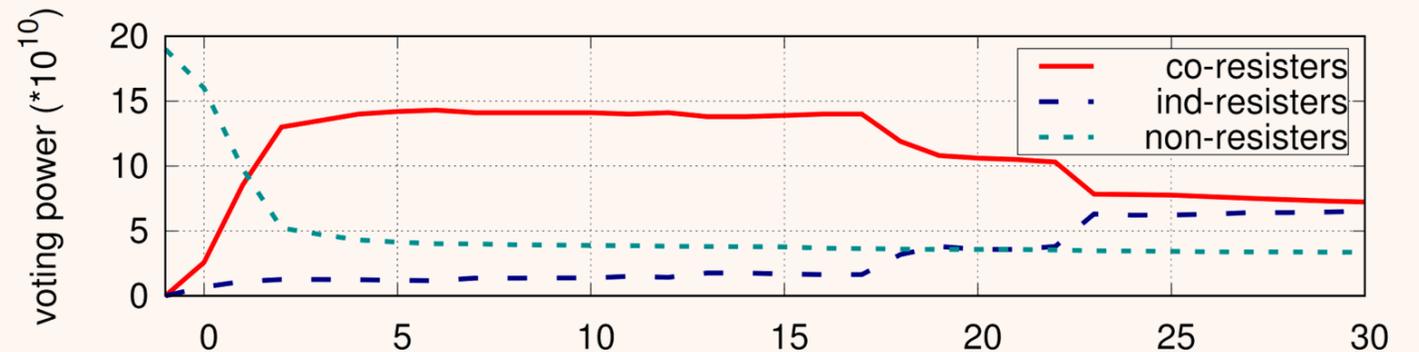
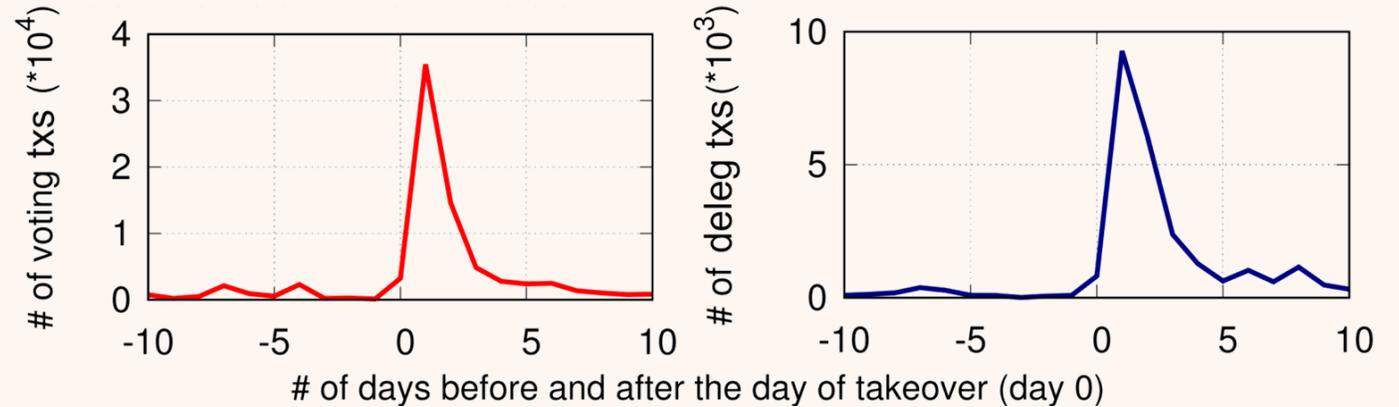
Either PROXY ME <https://beta.steemconnect.com/sign/account-witness-proxy?proxy=theycallmedan&approve=1>

Or VOTE HERE: <https://steemitwallet.com/~witnesses> VOTE FOR 22-42 at a minimum, we need to vote for the same witnesses to maximize our votes! USE ALL 30 OF YOUR VOTES!

MAKE SURE YOU ARE NOT VOTING FOR SOCK PUPPET ACCOUNTS!



The Steem community actively responded.



The Effect of Resistance

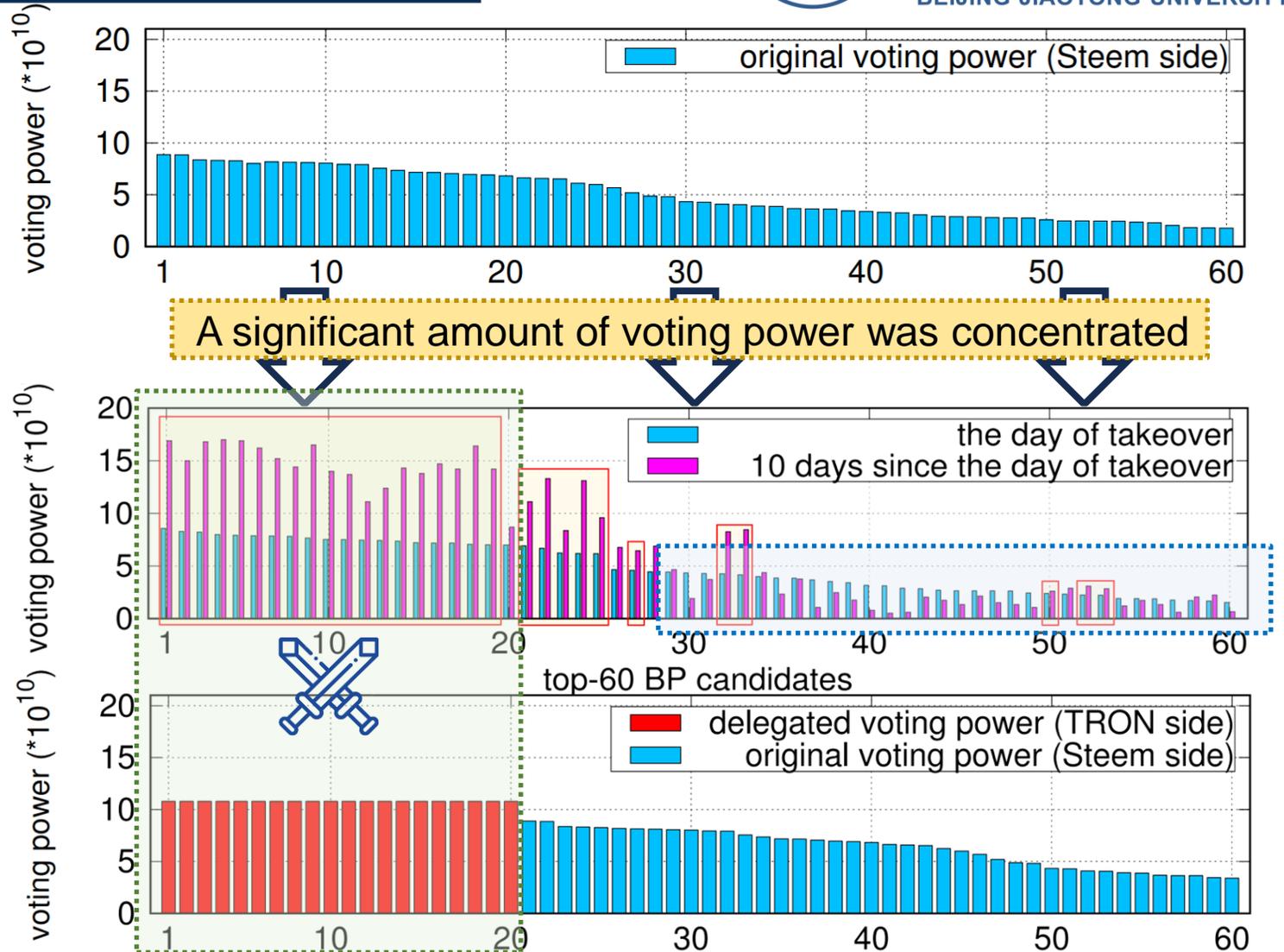


北京交通大学

BEIJING JIAOTONG UNIVERSITY

■ All the candidates suggested by the call-to-action witnessed positive growth in voting power, emerging as the core members countering the takeover.

■ In contrast, the majority of candidates not endorsed in the call-to-action experienced a decrease in their voting power.

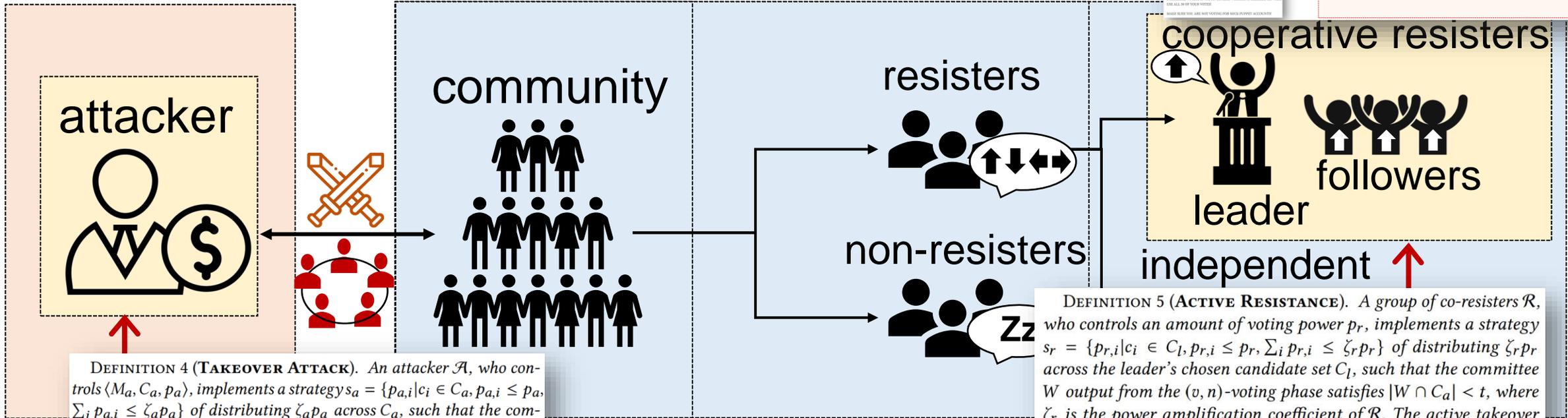




04

Takeover Resistance

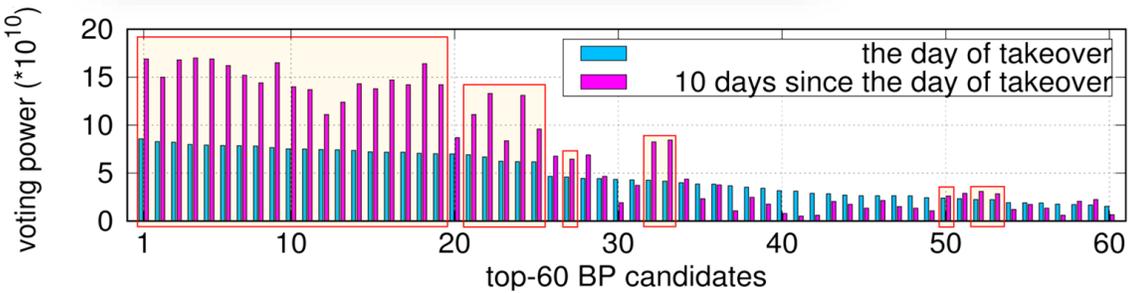
Active Resistance



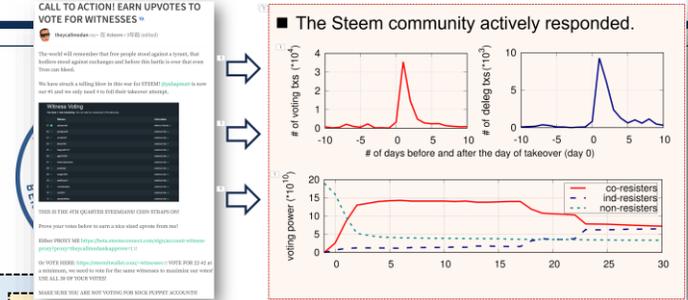
DEFINITION 4 (TAKEOVER ATTACK). An attacker \mathcal{A} , who controls $\langle M_a, C_a, p_a \rangle$, implements a strategy $s_a = \{p_{a,i} | c_i \in C_a, p_{a,i} \leq p_a, \sum_i p_{a,i} \leq \zeta_a p_a\}$ of distributing $\zeta_a p_a$ across C_a , such that the committee W output from the (v, n) -voting phase satisfies $|W \cap C_a| \geq t$, where ζ_a is the power amplification coefficient of \mathcal{A} .

DEFINITION 5 (ACTIVE RESISTANCE). A group of co-resisters \mathcal{R} , who controls an amount of voting power p_r , implements a strategy $s_r = \{p_{r,i} | c_i \in C_l, p_{r,i} \leq p_r, \sum_i p_{r,i} \leq \zeta_r p_r\}$ of distributing $\zeta_r p_r$ across the leader's chosen candidate set C_l , such that the committee W output from the (v, n) -voting phase satisfies $|W \cap C_a| < t$, where ζ_r is the power amplification coefficient of \mathcal{R} . The active takeover resistance, denoted as R_A , is quantified as the minimum amount of voting power p_a an attacker \mathcal{A} needs to defeat the co-resisters and successfully take over the target blockchain.

Active Resistance



When resistance is led by co-resisters, how can the voting system be designed to maximize the effectiveness of active resistance?



Active Resistance



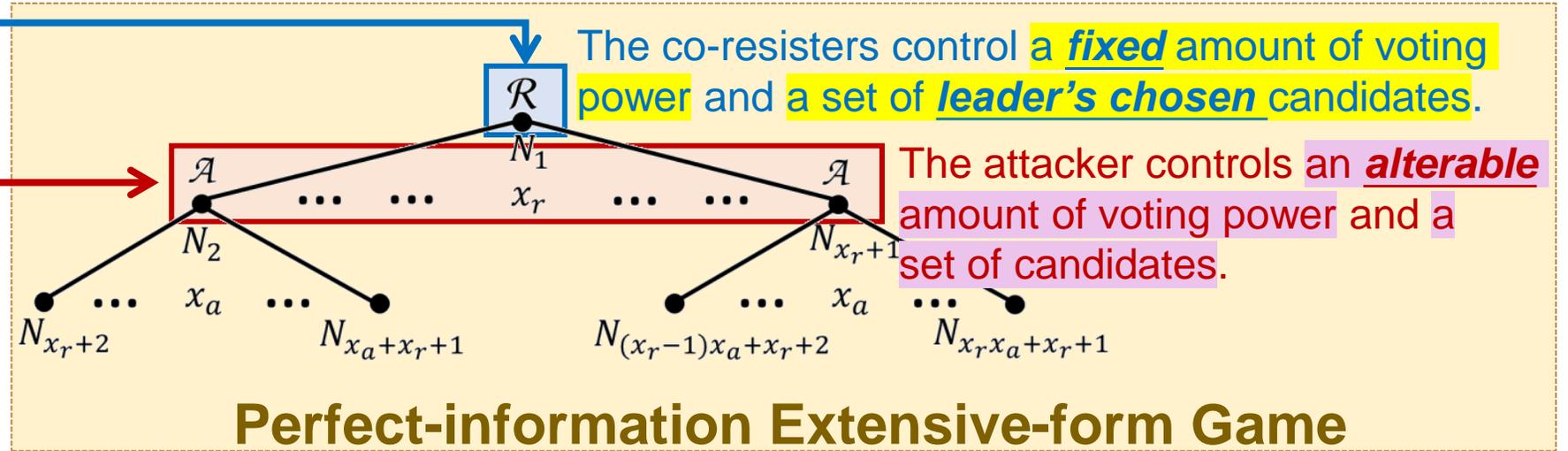
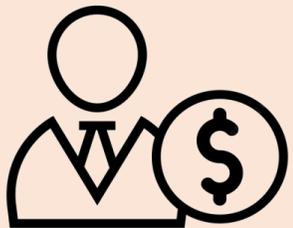
北京交通大学

BEIJING JIAOTONG UNIVERSITY

cooperative resisters



attacker



THEOREM 1. (\hat{s}_a, \hat{s}_r) is the subgame-perfect Nash equilibrium.

LEMMA 2. \hat{s}_r is the best response of \mathcal{R} to \hat{s}_a .

LEMMA 3. On the equilibrium path induced by \hat{s}_r and \hat{s}_a together,

LEMMA 4. Given a pair of parameters (t, n) such that $\frac{2}{3}n < t < n$, by setting the MaxVote parameter $v \leq n - t + 1$, the active takeover

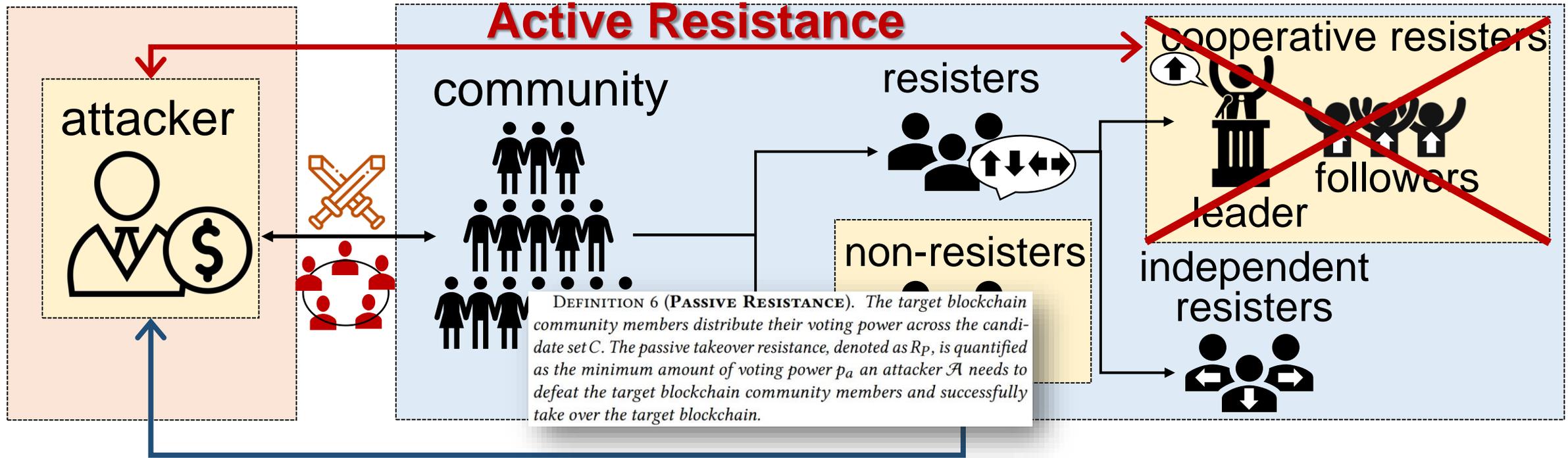
THEOREM 2. In an approval-voting supermajority-governing sys-

LEMMA 5. Given a pair of parameters (t, n) , by setting the MaxVote parameter $v = n - t + 1$, the active takeover resistance R_A can reach the upper bound whether or not the players are communities that employ a minimum number of simple call-to-actions.

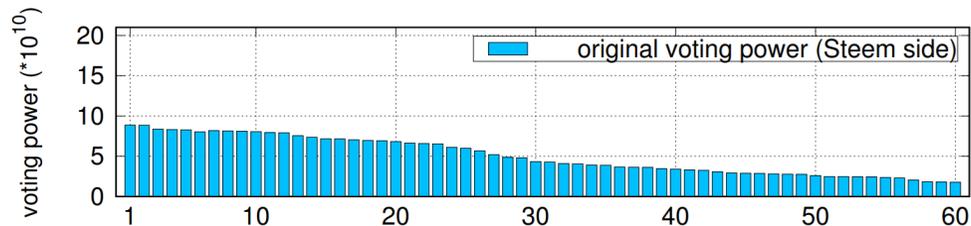
- We prove the existence of a **subgame-perfect Nash equilibrium**.
- We demonstrate the existence of an **upper bound for the active takeover resistance** of DPoS blockchains for both approval voting and cumulative voting.



Passive Resistance



Passive Resistance



When resistance is passive or the power of co-resisters is much lower than that of non-resisters, how can we understand actual voter preferences and based on them, how can we design a voting system to enhance the effectiveness of passive resistance?

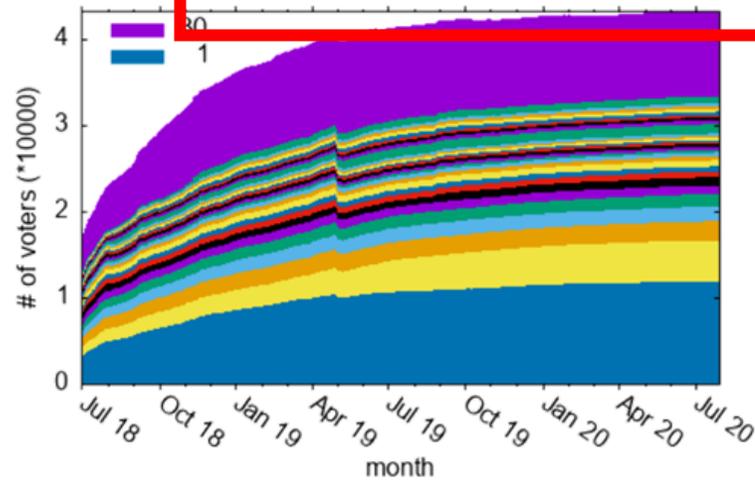


Passive Resistance

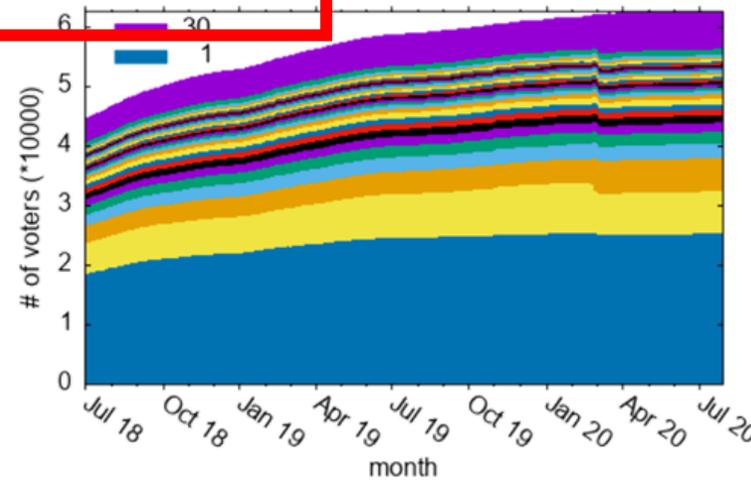
Reduce?

- The first large-scale empirical study on passive resistance in **EOSIO**, **Steem**, and **TRON**.

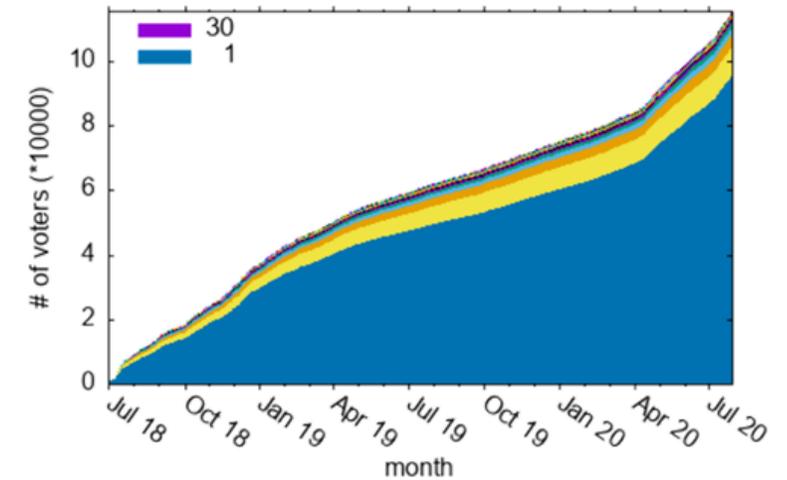
- Voters can cast up to 30 votes ($v=30$) but **how many votes were actually cast?**



(a) EOSIO



(b) Steem



(c) TRON

- Surprisingly, many voters chose to cast only a few or, in some cases, a single vote.
- It may be easier to understand the phenomenon in **TRON** because TRON adopts the cumulative voting rule so that voters cannot amplify their power by casting more votes.
- Nevertheless, we find that nearly half of **EOSIO** voters choose to cast fewer than 5 votes and more than half of **Steem** voters consistently cast fewer than 3 votes.

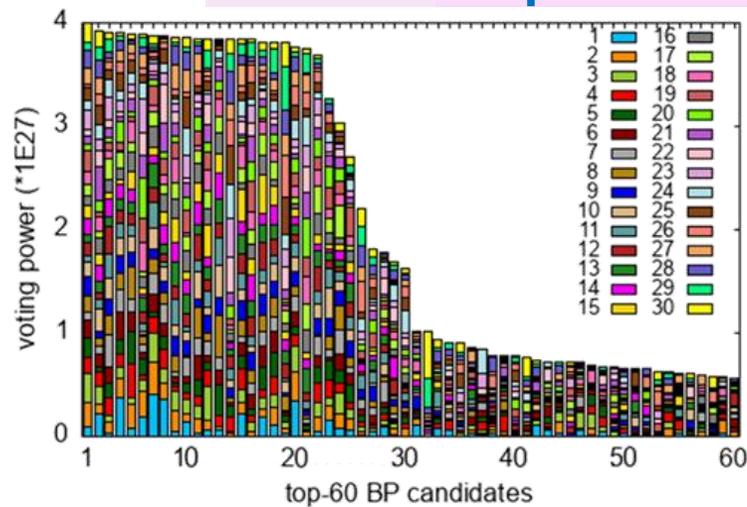
Not desirable from the perspective of protecting DPoS blockchains against takeovers.



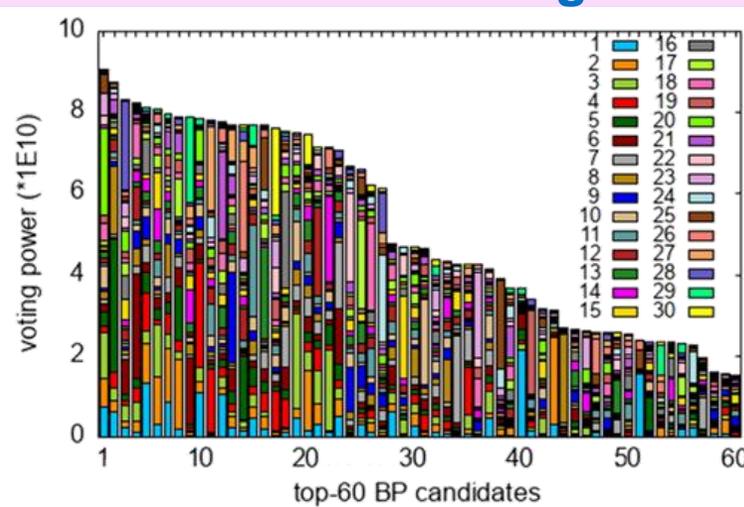
Passive Resistance

- The first large-scale empirical study on passive resistance in **EOSIO**, **Steem**, and **TRON**.

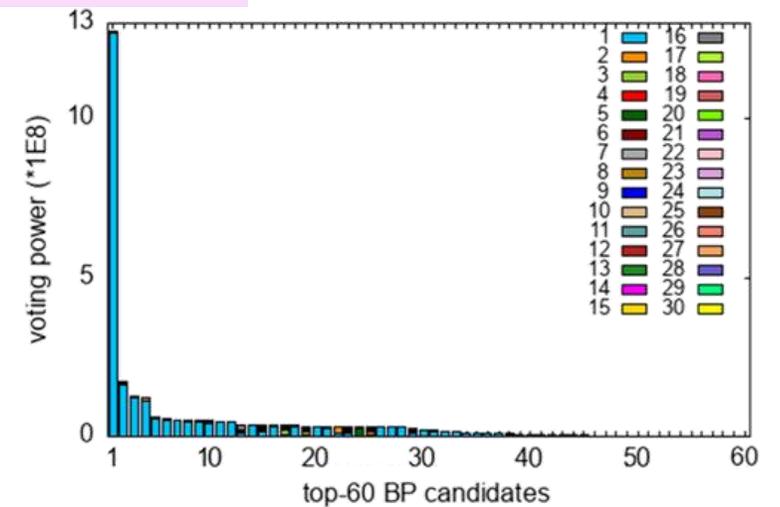
➤ What are the **priorities that voters would assign to candidates?**



(a) EOSIO



(b) Steem



(c) TRON

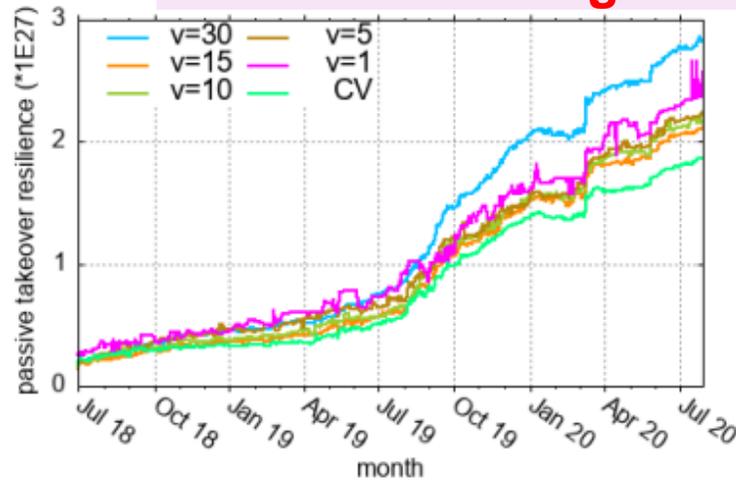
- In **EOSIO**, voters tended to be highly inconsistent with the priorities assigned to candidates.
- In **TRON**, however, we find that the first candidate receives an overwhelming amount of voting power, over 7 times that of the second candidate.

The relatively even distribution of priorities in EOSIO may not be desirable for resisting takeovers.

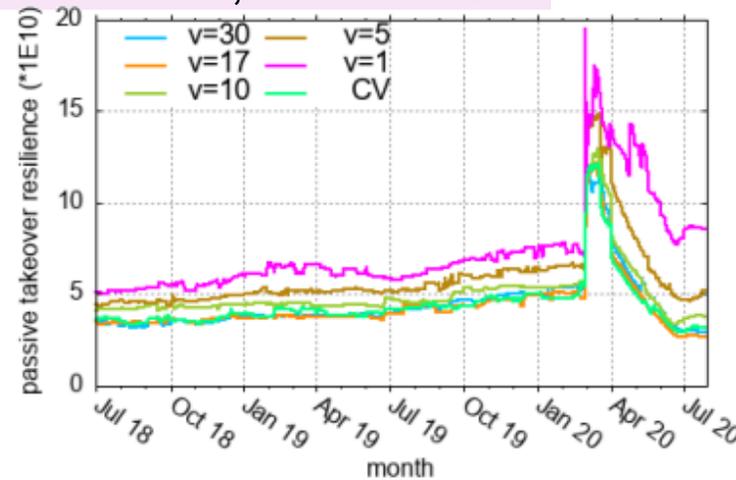


Passive Resistance

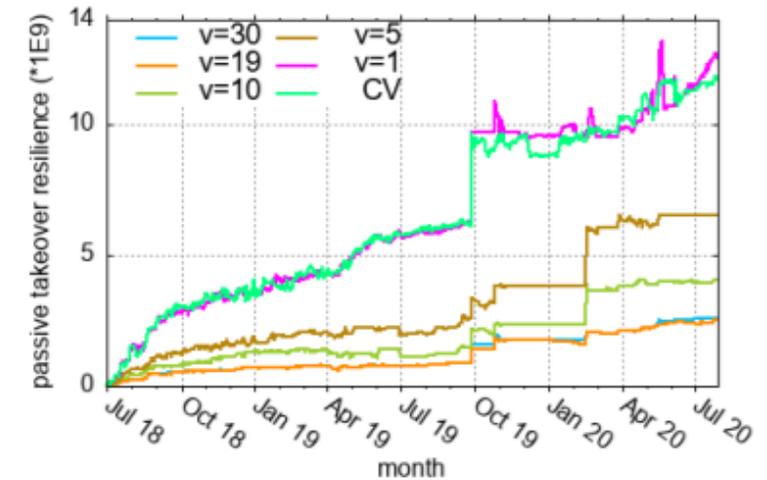
- Based on the actual voter preferences, we simulate the voting power distributions for **EOSIO**, **Steem**, and **TRON** when adopting different voting system design choices.
 - **Approval Voting** rule with a fixed pair of (t, n) and a MaxVote v varying from 30 to 1.
 - **Cumulative Voting** rule with $v = 30$, as in TRON.



(a) EOSIO



(b) Steem



(c) TRON

Our findings indicate that the approval voting rule with a small parameter v is a suitable choice for all three blockchains examined in this work, which may serve as a foundation for optimizing voting system design choices in diverse DPoS blockchain environments.



05

Conclusion

Conclusion



In this paper, we demonstrate that the resistance of a DPoS blockchain to takeovers is governed by **both** the **theoretical design** and the **actual use** of its underlying coin-based voting system.

Theoretically

- model the coin-based voting system
- formalize the takeover attack and resistance model
- model a takeover game between an attacker and the cooperative resisters and
- demonstrate the upper bound of active takeover resistance

Empirically

- present the first large-scale empirical study of the passive takeover resistance of EOSIO, Steem and TRON
- demonstrate the diversity of voter preferences, which significantly affects the passive takeover resistance when the parameters of the coin-based voting system change.

Our study suggests potential ways to improve the takeover resistance of DPoS blockchains, including the recommended configuration settings of the system based on our theoretical and empirical analyses.

We believe the study presented in this work provides novel insights into the security of coin-based voting governance and can potentially facilitate more future work on designing new voting rules for decentralized governance that provide more compliance with resistance to takeovers.

Conclusion

In this paper, we demonstrate that the resistance of a DPoS blockchain to takeovers is governed by **both** the ***theoretical design*** and the ***actual use*** of its underlying coin-based voting system.

Our study suggests potential ways to improve the takeover resistance of DPoS blockchains, including the recommended configuration settings of the system based on our theoretical and empirical analyses.

We believe the study presented in this work provides novel insights into the security of coin-based voting governance and can potentially facilitate more future work on designing new voting rules for decentralized governance that provide more compliance with resistance to takeovers.



北京交通大学

BEIJING JIAOTONG UNIVERSITY

Thanks!

li.chao@bjtu.edu.cn

Chao Li, Balaji Palanisamy, Runhua Xu, Li Duan, Jiqiang Liu, Wei Wang. “How Hard is Takeover in DPoS Blockchains? Understanding the Security of Coin-based Voting Governance.” ***ACM CCS 2023.***