"Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain"

Qitong Cao

Duke Kunshan University
CS/Econ 206 | Computational Economics

May 5 2022

1.Background and Motivation

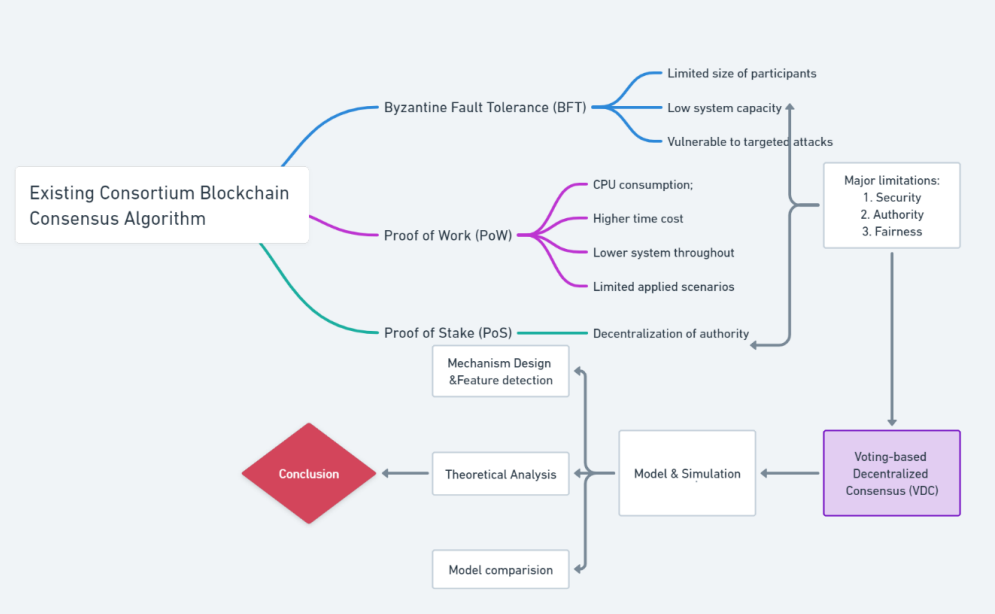

Figure 1: Summary Mindmap created by Whimsical

- Background
  - Limitations: high energy consumption, time inefficiency, low transaction throughput, poor security, poor user revenue fairness (Sun et al. 2020).

1.Background and Motivation

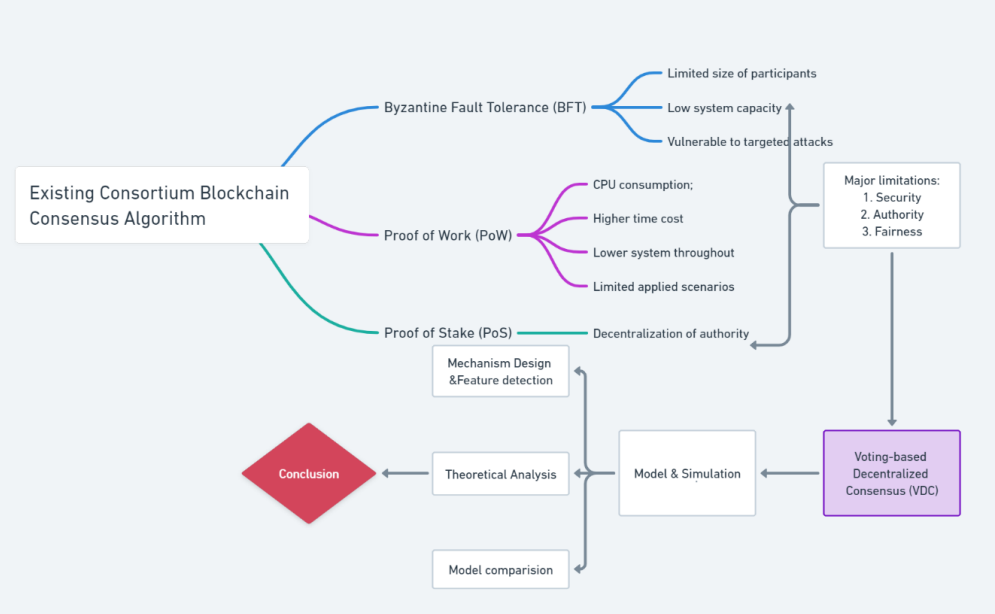

Figure 1: Summary Mindmap created by Whimsical

- Background
  - Limitations: high energy consumption, time inefficiency, low transaction throughput, poor security, poor user revenue fairness (Sun et al. 2020).
- Motivation
  - To improve the efficiency and security of the consortium blockchain to and the performance of the blockchain platform.

Research Question

- Research Questions: How to improve the efficiency and security of consortium blockchain?

Methods

Model & Simulation method

- Authority: by increasing uncertainty
- Security: by introducing "lottery drawing" to avoid attacks
- Regulation: by adding "asset" to increase "crime cost"

||

Model Comparison

- Compare with Practical Byzantine Fault Tolerance (PBFT) and Mixed Byzantine Fault Tolerance (MBFT) algorithms
- shows apparent advantages in user benefit fairness, time efficiency, and elasticity against target attack and has acceptable extra cost in energy consumption.

Intellectual Merits

Proof of Work (PoW)

the cost of additional CPU consumption; higher time cost; lower system throughput;the quality of service requirements of some scenarios (Frankenfield 2021).

- increase the cost of malicious behavior

Intellectual Merits

Proof of Work (PoW)

the cost of additional CPU consumption; higher time cost; lower system throughput;the quality of service requirements of some scenarios (Frankenfield 2021).

- increase the cost of malicious behavior

Proof of Stake (PoS)

the decentralization of authority

- converted identities to limit and disperse authority to avoid monopoly

Intellectual Merits

Proof of Work (PoW)

the cost of additional CPU consumption; higher time cost; lower system throughput;the quality of service requirements of some scenarios (Frankenfield 2021).

- increase the cost of malicious behavior

Proof of Stake (PoS)

the decentralization of authority

- converted identities to limit and disperse authority to avoid monopoly

Byzantine Fault Tolerance (BFT) algorithm

low system capacity; leaders vulnerable to targeted attacks

- utilize the unpredictability against the targeted attacks

Practical Impacts

- The new consensus algorithm is expected to solve the drawbacks of the existing blockchain algorithms or update the current consensus algorithm to improve the performance of the blockchain platform.
- As a newly born partial theoretical algorithm mechanism, VDC also needs further experiments and improvements to adapt to highly complex application scenarios (Sun et al. 2020).

Critics

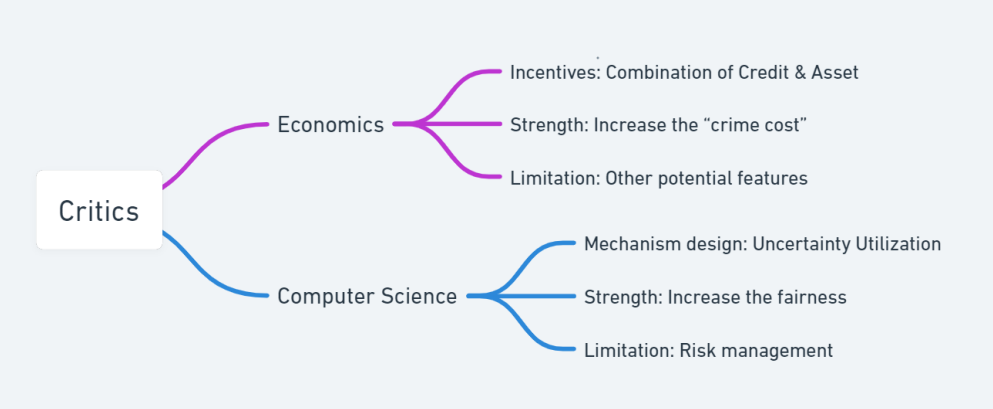

Figure 2: Critics Mindmap created by Whimsical

- Economics for Computer Science
  - Incentives: Combination of Credit & Asset
  - Strength: Increase the "crime cost"
  - Limitation: Other potential features

Critics

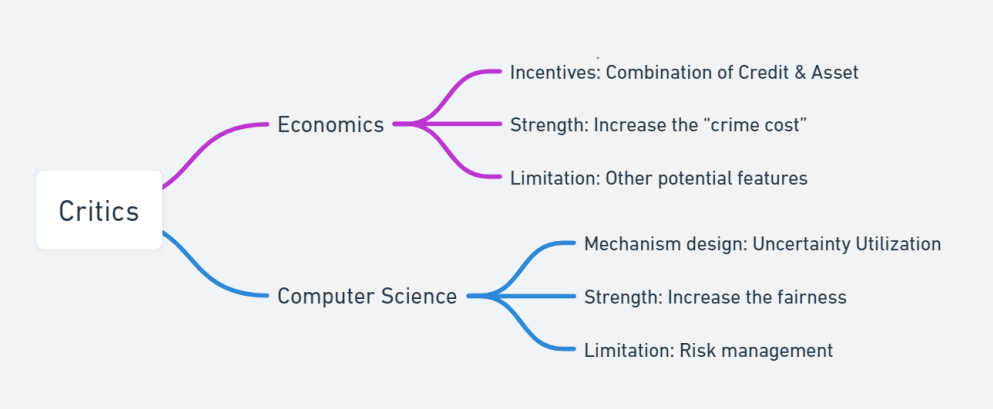

Figure 2: Critics Mindmap created by Whimsical

- Economics for Computer Science
  - Incentives: Combination of Credit & Asset
  - Strength: Increase the "crime cost"
  - Limitation: Other potential features
- Computer Science for Economics
  - Mechanism design: Uncertainty Utilization
  - Strength: Increase the fairness
  - Limitation: Risk Management

Inspirations

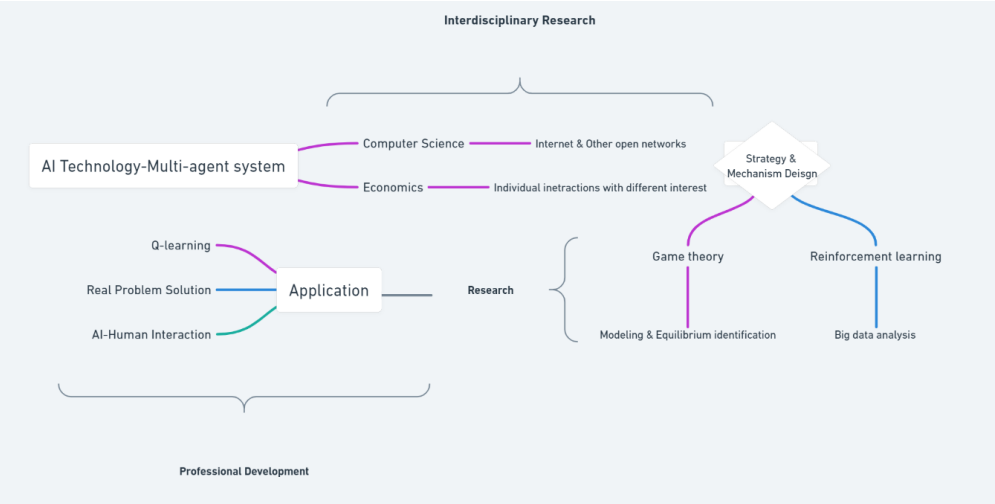

Figure 3: Inspirations Mindmap created by Whimsical

- Interdisciplinary Research
  - Interactions with other non-human agents

Inspirations

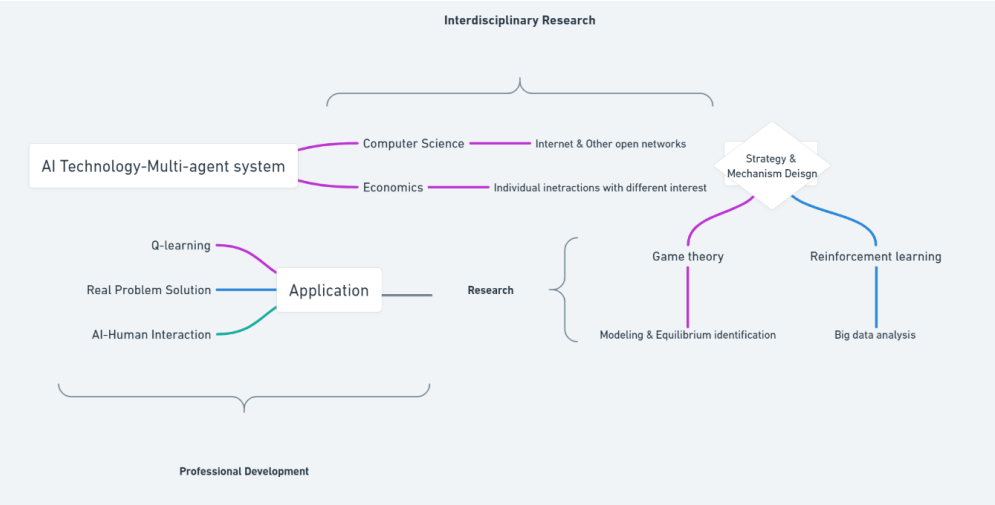

Figure 3: Inspirations Mindmap created by Whimsical

- Interdisciplinary Research
  - Interactions with other non-human agents
- Research for Real-world Practices
  - Game Theory Model Construction
  - Reinforcement learning with big data

Inspirations

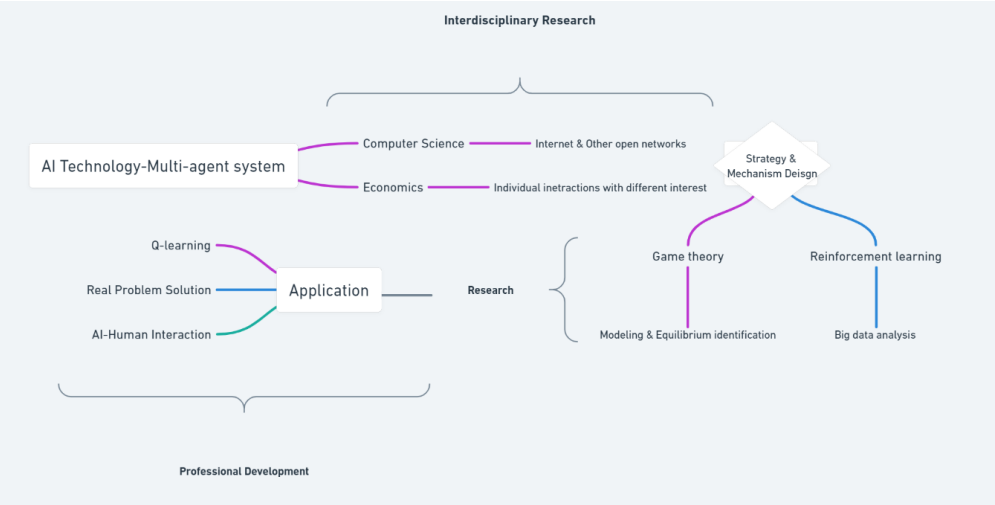

Figure 3: Inspirations Mindmap created by Whimsical

- Interdisciplinary Research
  - Interactions with other non-human agents
- Research for Real-world Practices
  - Game Theory Model Construction
  - Reinforcement learning with big data
- Future Professional Growth
  - Applications: content ranking in user-generated content sites

Revision responding to peer review

- Jargon Explanation
  - Definition of technical words added to the article
  - Glossary table of major words construction
  - Abbreviations spelled out
- More citations
  - Citations of major technical words
  - Citations in "Background" and "Intellectual Merits"
- Revision of "Professional Development"
  - Original part moved to Part II
  - More related topic added

Bibliography (Major Reference)

- Website
  - Consortium Blockchain | CoinMarketCap. n.d. CoinMarketCap Alexandria. Accessed May 5, 2022.
  - Frankenfield, Jake. 2019a. Consensus Mechanism (Cryptocurrency). Investopedia. 2019.
  - Practical Byzantine Fault Tolerance (PBFT) - BitcoinWiki. n.d. En.bitcoinwiki.org. Accessed May 5, 2022.
- Articles
  - Dafoe, Allan, Yoram Bachrach, Gillian Hadfield, Eric Horvitz, Kate Larson, and Thore Graepel. 2021. Cooperative AI: Machines Must Learn to Find Common Ground. Nature 593 (7857): 3336.
  - Daly, Lyle. 2021. What Is Byzantine Fault Tolerance? The Motley Fool. November 10, 2021.
  - Daly, Lyle. 2021. What Is Byzantine Fault Tolerance? The Motley Fool. November 10, 2021.
  - Du,Mingxiao, Qijun Chen, and Xiaofeng Ma. 2020. MBFT: A New Consensus Algorithm for Consortium Blockchain. IEEE