

# ブロックチェーン公開講座 第12回

## DApps・エコノミクス設計入門

---

トークンの価値づけやインセンティブの設計

伊東謙介

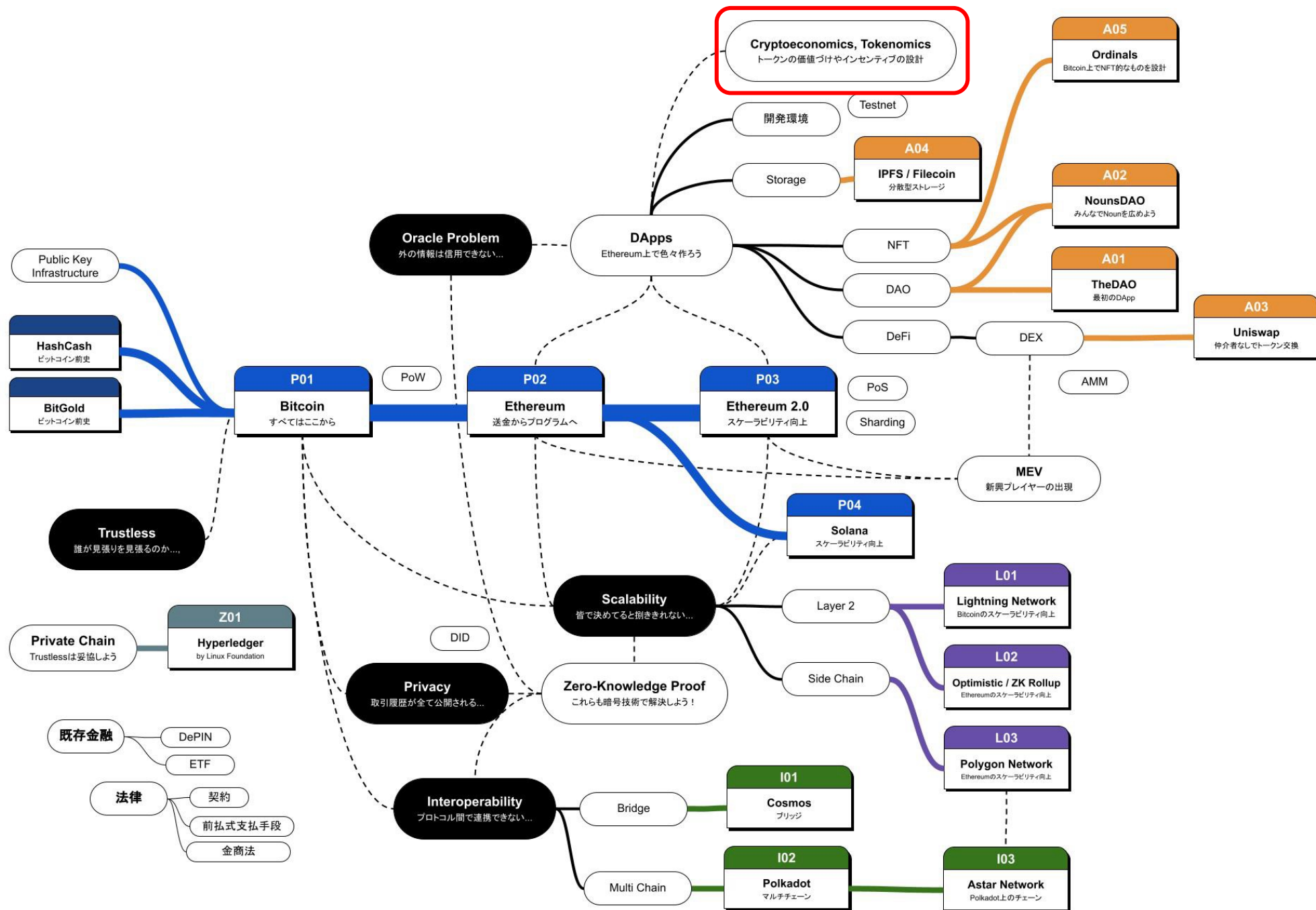
東京大学ブロックチェーンイノベーション寄付講座

特任研究員

k-ito@g.ecc.u-tokyo.ac.jp







## これはどのような講義？

- **Cryptoeconomics, Tokenomics** の観点でプロトコルやDAppsを解釈する
  - **なぜ？**: 自律分散的な仕組みを設計する上で、暗号に並んで有用な概念だから
  - What や Why ではなく How の部分
  - How の中でも大工さんよりは建築家に近い部分
- 先にBitcoin Protocol, Ethereumに関する講義を受講することを推奨します
  - Bitcoin Protocolの大まかな設計を把握している前提で講義します（詳細まで抑えている必要はありません）
- **仕様の説明が終わったのでようやく解釈の話が行えます！**
  - 前提として最初にどうしても仕様の話が必要だった
  - 設計の解釈は、Discordなどでもぜひ議論したいと思っています
- この講義は以下の論文に基づいています
  - Ito (2024), [Cryptoeconomics and Tokenomics as Economics: A Survey with Opinions](#), In *International Conference on Blockchain 2024*.
  - 講義で紹介している具体例や研究の詳細・出典はこの論文の参考文献をご参照ください



## これはどのような講義？

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
3. 分散性のための合意形成を設計する
4. 自律性のためのトークン価値を設計する
5. ケーススタディ
6. まとめ



# 1. イントロダクション

---

なぜ Cryptoeconomics, Tokenomics は重要なのか？

# Bitcoin Protocolの新規性はインセンティブ設計の活用にある

- "Peer-to-peer electronic cash system" はBitcoin Protocol以前も試みられていた
  - e.g., b-money (1998), Bit gold (2005)
- しかし「ピアたちの間で取引記録の意見が割れた場合にどう決着を付けるか？」について効果的な解決策がなかった
  - ピアの数がどれくらいかわからない
  - ピアは戦略的に嘘の報告をするかもしれない
  - 戦略的でなくとも、ピアが故障して通信に失敗することもある
  - このような環境で「正しい」取引記録をどのように決めれば良いのだろうか...
- Bitcoin Protocolは「**インセンティブ設計の活用**」という先例とは違ったアプローチを用いてこの問題を（実用的なレベルでは）解決した

\* ただしBitcoin Protocolにはファイナリティがないため、厳密には解決したとは言えない (quasi-solution)



# Bitcoin Protocolの新規性はインセンティブ設計の活用にある

## *Main Rules of the Bitcoin Protocol*

- Transaction records are sequentially stored in blocks, and peers maintain an identical chain of blocks through consensus-building (*blockchain*).
- Peers can create a new block and attach it to any existing block in the chain; however, the success of this task is probabilistic, directly proportional to the relative amount of computing resources expended by the peer (*proof-of-work* [6], [7]).
- In the event of a chain fork into multiple paths, the longest chain is accepted as the consensus (*Nakamoto consensus*).
- Peers who successfully create a block in the longest chain receive newly minted Bitcoins as rewards (*coinbase as contribution rewards*).

嘘が付けないというよりも、嘘を付くことが得にならない設計





## この新規性は後続にも継承されている

---

- *Ethereum* (2014)
  - 合意形成の対象を送金記録からプログラムの実行結果 (状態の遷移) へと一般化した
- *The DAO* (2016)
  - Ethereum上で作られた最初のDApps
  - Etherを用いた分散型投資ファンド

\*設計の脆弱性を突かれて、プールしていたetherが盗まれるという事件を引き起こした (EthereumとEthereum Classicに分派する原因)
- その他さまざまなDApps

## Cryptoeconomics, Tokenomicsはこの新規性を指す

---

- 2014-2016年に使われ始めるようになった用語
- 定義でなく目的で捉えるならば、これらの用語は「インセンティブ設計の活用」というBitcoin Protocolの新規性が扱う対象をon-chainの取引記録からより一般的な情報へ拡張しようとするものである

## しかしまだ課題が存在する

**Nick Szabo**

@NickSzabo4

An economist or programmer who hadn't studied much computer science, including cryptography, but guesses about it, cannot design or build a long-term successful cryptocurrency. A computer scientist and programmer who hasn't studied much economics, but applies common sense, can.

1:14 PM · Mar 23, 2018

**392** Reposts   **44** Quotes   **1,666** Likes   **23** BookmarksSource: <https://x.com/NickSzabo4/status/977035747713675264>, accessed September 4, 2023.

Cryptoeconomics, Tokenomicsは未だに (i)定義が曖昧かつ (ii)経済学との間に断絶が存在する



# お疲れ様でした！

## 1. イン트로ダクション

- Bitcoin Protocolの新規性はインセンティブ設計の活用にある
- この新規性は後続にも継承されている
- Cryptoeconomics, Tokenomicsはこの新規性を指す
- しかしまだ課題が存在する

2. 用語の歴史とそれに対する伊東の意見

3. 分散性のための合意形成を設計する

4. 自律性のためのトークン価値を設計する

5. ケーススタディ

6. まとめ



## 2. 用語の定義とそれに対する伊東の意見

---

Cryptoeconomics, Tokenomicsとは何か？どうあるべきか？



# Cryptoeconomicsの歴史

Ethereum FoundationのVlad Zamfirが2015年のプレゼンテーションで以下のように言及

- *“a formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.”*

同年にVitalik Buterinがcryptoeconomicについて以下のように言及

- *“it’s decentralized, it uses public key cryptography for authentication, and it uses economic incentives to ensure that it keeps going and doesn’t go back in time or incur any other glitch.”*

少し遅れて学術的にも言及されるようになる

- *“a branch of mechanism design, which is a branch of microeconomics”* (Davidson 2016)
- *“It has more in common with mechanism design—an area of mathematics and economic theory, sometimes referred to as reverse game theory”* (Obasi 2017)
- *“Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies”* (Brekke and Alsindi 2021)

# Cryptoeconomicsの歴史

Ethereum FoundationのVlad Zamfirが2015年のプレゼンテーションで以下のように言及

- “a formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.”

同年にVitalik Buterinがcryptoeconomicsについて以下のように言及

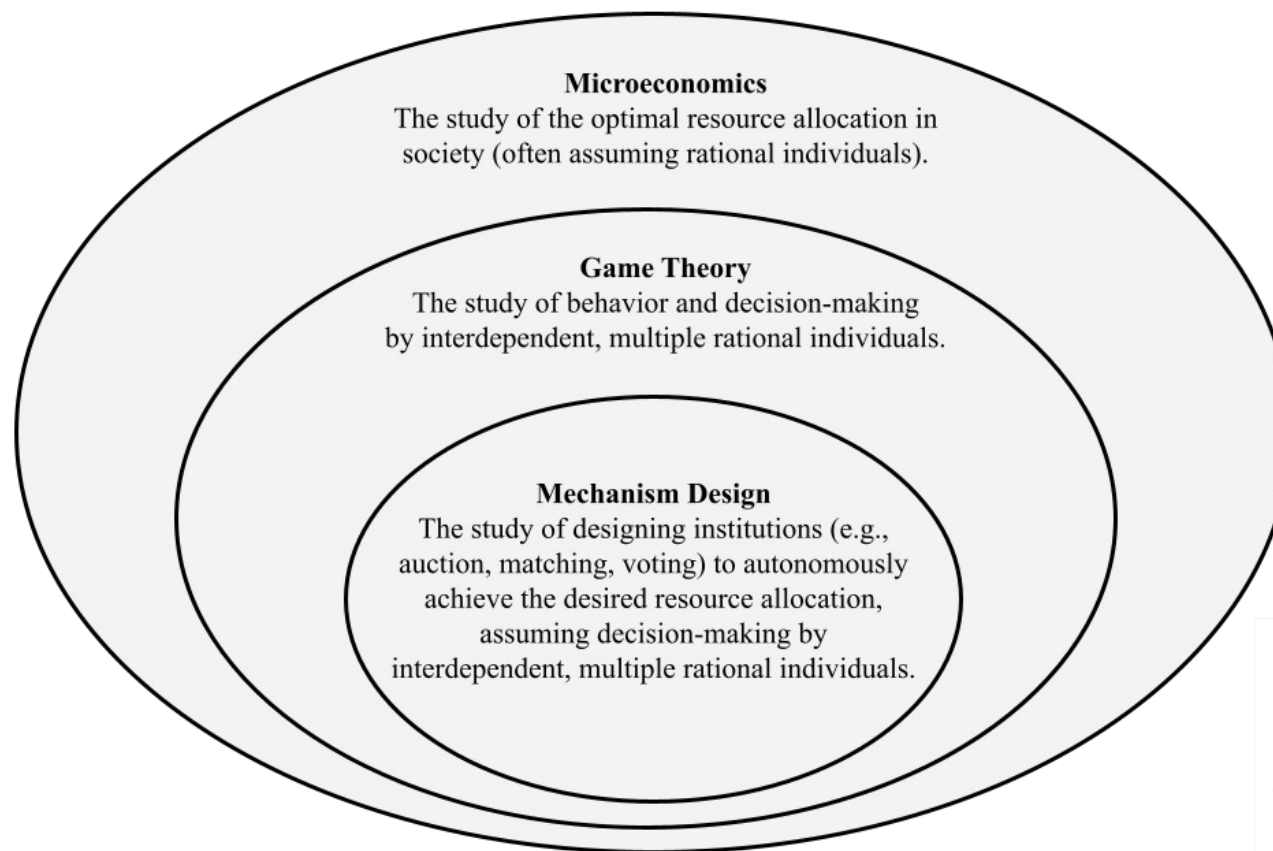
- “it’s decentralized, it uses economic incentives to ensure that it keeps

意見集約 (合意形成) の手段としてインセンティブ設計を活用すること、学術的にはメカニズムデザインに位置づけられる

少し遅れて学術的にも

- “a branch of mechanism design (Obasi 2016)
- “It has more in common with mechanism design—an area of mathematics and economic theory, sometimes referred to as reverse game theory” (Obasi 2017)
- “Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies” (Brekke and Alsindi 2021)

# Cryptoeconomicsの歴史



補足: ミクロ経済学、ゲーム理論、メカニズムデザインの関係性



# Tokenomicsの歴史

Tokenomicsという用語自体は少なくとも2012年には存在したが、ブロックチェーンの文脈で学術的に言及されるようになったのは2017年ころから

e.g.,

- “*the utility role of the token*” to “*deliver a viable business model for the long term*” (Mougayar 2017)
- “*(1) a means of self-funding within the crypto economy, (2) the deployment of a token within the ecosystem of an ICO project and (3) the set of all economic activity generated through the creation of tokens*” (Ennis, et al. 2018)
- “*the study of how crypto tokens are used within the blockchain ecosystem,*” which encompasses: “*1) The number of tokens issued and the way they are issued (vesting schedule, airdrops, etc.). 2) The economics of a consensus algorithm; largely referred to as crypto-economics. 3) The general structure of the system: game theoretic and economic incentives*” (Kampakis 2022)

# Tokenomicsの歴史

Tokenomicsという用語自体は少なくとも2012年には存在したが、ブロックチェーンの文脈で学術的に言及されるようになったのは2017年ころから

e.g.,

- “the utility role of the token” (Mougayar 2017)
- “(1) a means of self-governance within the ecosystem of a blockchain network” (Ennis, et al 2017)  
トークン価値設計の議論にはじまり、段々とCryptoeconomicsの領域も包含するようになる
- “the study of how cryptocurrencies work” (Kampakis 2022)  
encompasses: “1) The number of tokens issued and the way they are issued (vesting schedule, airdrops, etc.). 2) The economics of a consensus algorithm; largely referred to as crypto-economics. 3) The general structure of the system: game theoretic and economic incentives” (Kampakis 2022)



## 意見: どちらも学術的には先例が存在する

---

- Mechanism Design
  - *Algorithmic Mechanism Design* (Nisan et al, 1999)
    - *Distributed Algorithmic Mechanism Design* (Feigenbaum et al. 2000)



Cryptoeconomicsの先例 / メカニズムデザインと計算機科学の融合

## 意見: どちらも学術的には先例が存在する

メカニズムデザインを計算機科学の論点 (e.g., ルーティング, ロード  
balancing) に応用する

このとき、既存のメカニズムデザインでは考慮しない新しい制約  
(e.g., 計算資源) も扱う

- Mechanism Design
  - *Algorithmic Mechanism Design* (Nisan et al, 1999)
  - *Distributed Algorithmic Mechanism Design* (Feigenbaum et al. 2000)

アルゴリズムメカニズムデザインの中でも、エージェントや計  
算資源、ネットワークが分散しているPeer-to-peerシステムに焦点  
をあてる

Cryptoeconomicsの先例 / メカニズムデザインと計算機科学の融合



## 意見: どちらも学術的には先例が存在する

---

- “*Open Problem 10. Can digital signatures (or, more generally, cryptographic protocol-design techniques) always be used to convert a distributed algorithmic mechanism in which some of the parties must be assumed to be obedient into one with a more realistic strategic model?*” (Feigenbaum and Shenker 2004)
- “*Open Problem 18. Can one design monetary P2P systems that provide better performance than purely barter P2P systems? Can one characterize, in simple models, the possible outcomes achievable with both kinds of P2P economies?*” (Feigenbaum and Shenker 2004)





## 意見: どちらも学術的には先例が存在する

---

- 新古典派経済学 (特にモノの価値と価格に関する議論)
- 金融経済学 (特に金融商品や金融政策、デジタル通貨の設計)



Tokenomicsの先例 / オーソドックスな経済学が結構カバーしている

## 意見: どちらも学術的には先例が存在する

モノの価値は何によって決まるのか？

- **費用価値説:** モノを追加1単位供給することにどのくらいコストがかかるかによって決まる
  - 売り手としてはそのコストより高く売らないと利益が出ない
- **効用価値説:** モノを追加1単位需要することでどのくらい満足度が得られるかによって決まる
  - 買い手としてはその満足度より安く買えるならばどんどん買うはず

結局どうなのかというと... どちらも正しい

供給側の事情（前者）と需要側の事情（後者）が一致するところで価格が決まる

「価値の源泉が費用なのか効用なのかを議論することは、ハサミの上の刃と下の刃のどちらで紙を切っているのかを議論するようなものである」



Marshall (1890) の価値と価格に関する議論の整理 / Bitcoin Protocol実装の100年以上前！



意見: しかし両者を組み合わせる試みはまだ存在しない

## Cryptoeconomics

分散性のための合意形成の設計

合意形成は、報酬としてのトークンに価値がなければ自律的にならない

先例:

*Algorithmic Mechanism Design,  
Distributed Algorithmic Mechanism Design.*



## Tokenomics

自律性のためのトークン価値の設計

トークン価値は、システムが合意形成を扱わなければ分散性に貢献しえない

先例:

*新古典派経済学 (特に価値と価格の議論), 金融経済学  
(特に金融商品や金融政策、デジタル通貨の設計).*

Cryptoeconomics と Tokenomics は、統合してこそ新しい！

# お疲れ様でした！

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
  - Cryptoeconomicsの歴史
  - Tokenomicsの歴史
  - 意見: どちらも学術的には先例が存在する
  - 意見: しかし両者を組み合わせる試みはまだ存在しない
3. 分散性のための合意形成を設計する
4. 自律性のためのトークン価値を設計する
5. ケーススタディ
6. まとめ



### 3. 分散性のための合意形成を設計する

---

決め方の設計において何に気をつけるべきか？

## どのように戦略的行動に対処するか？

戦略的行動とは *the action of deliberately misreporting accurate information* である

- Bitcoin protocolのピアは矛盾するトランザクション(e.g., 二重支払い)を含むブロックを作成するかもしれない
- The DAOの利用者は自分の提案により多くのetherを集めるために適切な投資先を誤報告するかもしれない

### ブロックチェーンの文脈ではどのように対処しているのか？

- Bitcoin protocol: PoWとNakamotoコンセンサスで合意形成を計算資源による多数決投票にした
- 多くのDApps: **Token-staking**を採用 (e.g., The DAO, Nouns DAO) し、合意形成をトークンによる多数決投票にした
  - EthereumのPoSとGasperの組み合わせもToken-stakingの一種と捉えられるかもしれない

#### *Token Staking (a simple example of binary choice)*

- Peers can stake any amount of their tokens to either *accept* or *reject* a proposal,
- Consensus is the choice of which collects more tokens after a certain period,
- All staked tokens are redistributed among peers who staked them on the consensus side.

# どのように戦略的行動に対処するか？

## 経済学の文脈ではどのように対処しているのか？

- まずは戦略的行動といくつかの規範 (これを満たせたら良いよねという条件) を定式化
  - Strategy-proofness (truthfulness): メカニズムのプレイヤーが本当の信念と異なる報告をすることで効用を増やすことが出来ない状態 \*ただし正直な報告と他の(虚偽)報告の効用が同じ場合も含む (i.e., truth-tellingが弱支配戦略になっている)
- 次にメカニズム自体の定式化
  - VCGメカニズム: strategy-proofnessを含む複数の規範を満たすことが出来るメカニズム
- こうした議論において、DAppsの設計に最も重要な概念はおそらく「**ケインズの美人投票**」である
  - 「この中から最も美人だと思う人に投票してください。最も票を集めた人に投票した方には賞金を出します」
  - プレイヤーは、自分の信念ではなく「他のプレイヤーの信念の予想」に基づいて投票を行ってしまう
  - こうなるとプレイヤーたちの信念が抽出できなくなる (選択肢の数だけナッシュ均衡が存在する)
- Bitcoin ProtocolにせよEthereumにせよToken-stakingにせよ「合意結果の選択肢を支持していた者には報酬を与える」という仕組みを採用した時点で美人投票の問題が発生してしまう
- しかし実際にはToken-stakingベースの仕組みがDApps設計では現状良く使われている
  - **なぜ？**: 後述する他の課題 (スパム・シビル攻撃・ただ乗り問題) に対して有効だから
  - **なぜ？**: それでもユニークなナッシュ均衡 (Schelling points) が得られるという主張もあるから

## どのようにスパム・シビル攻撃に対処するか？

スパムとは “*the act of spreading unsolicited and unrelated content* (Hayati, et al. 2010)” である

シビル攻撃とは “*the forging of multiple identities* (Douceur 2002)” である

- The DAOの利用者は大量の無意味な提案をして合意形成を混乱させたり、同じ主体が管理する異なるアドレスを複数人で管理しているふりをするかもしれない

### ブロックチェーンの文脈ではどのように対処しているのか？

- スパムに対しては「各トランザクションに対して小さなコストを課す」という伝統的な手法が一般的
  - Transaction fees (Bitcoin protocol, Ethereum)
  - Proposal fees (e.g., The DAO, Nouns DAO)
- シビル攻撃に対しては「投票力を個人やアカウントとは独立した指標にする」という手法が一般的
  - PoW: 1CPU = 1票
  - Token-staking (PoS含む): 1トークン = 1票
- あるいはより直接的に1人1票を担保する試みも存在する
  - Gitcoin: 複数のSNSアカウントを提出させることで個人とアカウントの一対一对応を (できるだけ) 担保
  - Worldcoin: 虹彩を用いた生体認証

# どのようにスパム・シビル攻撃に対処するか？

---

## 経済学の文脈ではどのように対処しているのか？

- 伊東が知る限りあまり積極的には研究されていない
- ゲーム理論的なモデル化や分析が行われてはいる
  - スパム: spammerとdetector間のゲーム (Androutsopoulos 2005, Reshef and Solan 2006, Rao and Reiley 2012)
  - シビル攻撃: (Gatti et al. 2004, Margolin and Levine 2007, Kumer and Bhuyan 2020)
- こうした分析は、報酬やペナルティ、トランザクションコストの効果を理論的に検証している





## どのようにただ乗り問題に対処するか？

ただ乗り問題とは “*an individual user who uses the system resources without contributing anything to the system* (Ramaswami and Liu 2003)” である

\* 経済学における使われ方と若干異なる点に注意

- たとえ戦略的行動やスパム・シビル攻撃対策が出来たとしても、信念を報告する時間や労力を考慮すると、私たちはそもそも合意形成に参加しなかったり、適当に同じ報告を行ったりするかもしれない

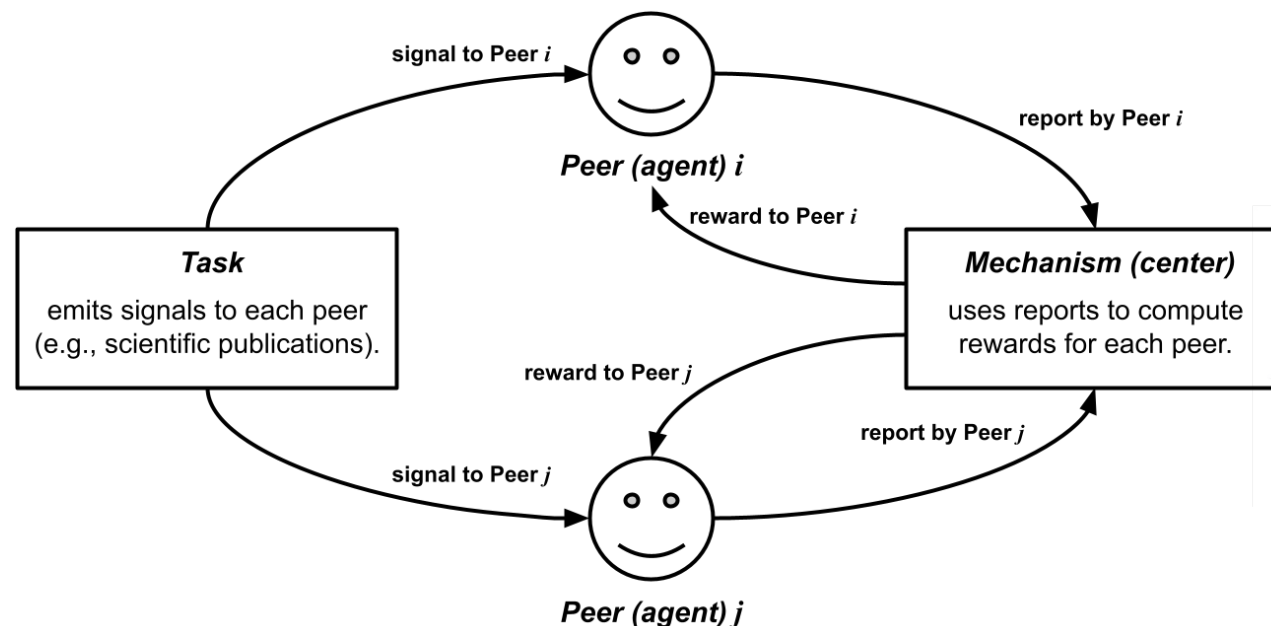
### ブロックチェーンの文脈ではどのように対処しているのか？

- 「合意結果の選択肢を支持していた者には報酬を与える」
  - トークンを新規発行 (Bitcoin protocol, Ethereum)
  - トークンを再分配 (Token-staking) \* 個人的にはゼロサムゲームなのでインセンティブにならないのでは？と思っている
- しかし先述のとおり、この方法だと美人投票の問題が発生する
- かといって合意形成の参加者全員に報酬を提供してもただ乗り問題は解決できない
  - 報酬目当てに適当な報告を行う可能性がある
- どうすれば良いのだろうか...

## どのようにただ乗り問題に対処するか？

### 経済学の文脈ではどのように対処しているのか？

- 一般的なメカニズムデザインの文脈では (伊東が知る限り) カバーしていない
  - 投票やオークションの研究はプレイヤーが報告を行うことが暗黙の前提になっている
  - 情報の抽出というよりも集約を研究している
- しかし、Distributed Algorithmic Mechanism Designの文脈では関連する研究が行われてきた
  - レーティング (e.g., amazonのレビュー) などにおいて正直な信念を抽出させるための報酬システムの設計
  - 情報の集約というよりも抽出を研究している “Information Elicitation without Verification”



# どのようにただ乗り問題に対処するか？

## 経済学の文脈ではどの

- 一般的なメカニズム
  - 投票やオークション
  - 情報の抽出
- しかし、Distributed A
  - レーティング (e
  - 情報の集約とい

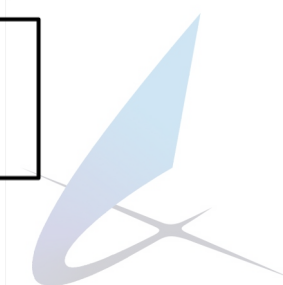
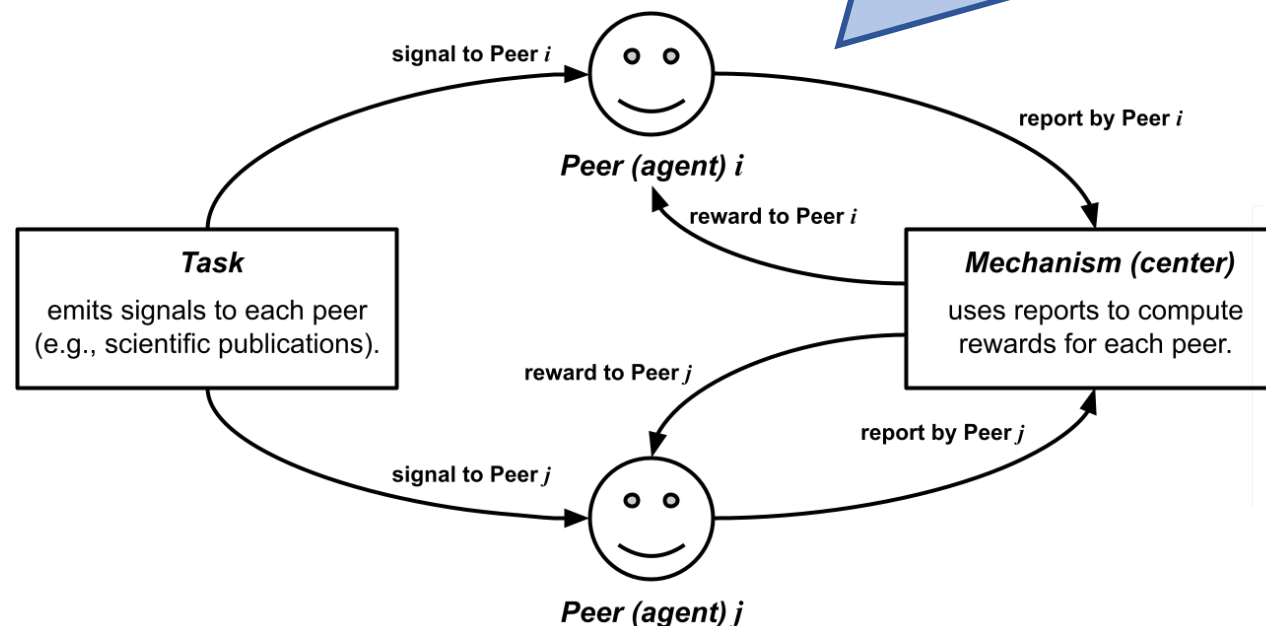
ピアたちは

- 割り当てられたタスクから確率的に発せられるシグナルを報告する
- 集まった報告を元に量が計算される報酬を受け取る

「受け取ったシグナルを正直に報告した場合に獲得する報酬量の期待値が最大になる」ようなメカニズムの設計を目指している

メカニズムには *Bayesian Truth Serum*, *Peer-prediction*, *Correlated Agreement* などの種類が存在する

システムの設計



## どのようにただ乗り問題に対処するか？

### 例: Dasgputa and Ghosh (2013) による Correlated Agreementモデル

- 2人の研究者  $i, j$ , がそれぞれ複数の論文 (タスク) をレビューするとする
- 彼らは binary signals, e.g., {accept, reject}, を報告するものとする
- $i, j$ , が同じ論文をレビューするたびに、彼らは以下の式で計算される報酬を受取る

reward term

$\delta$  (その論文に対する  $i$  の報告, その論文に対する  $j$  の報告) –  $\delta$  ( $i$ 's report randomly picked from her previous ones,  $j$ 's report randomly picked from her previous ones)

penalty term

このとき、 $\delta$  はクロネッカーのデルタである

$$\delta(a, b) = \begin{cases} 0 & \text{if } a \neq b, \\ 1 & \text{if } a = b. \end{cases}$$



## 他の規範にはどのようなものがあるか？

戦略的行動、スパム・シビル攻撃、ただ乗り問題、に対処すること以外にも、ブロックチェーンの文脈は合意形成に対して様々な規範を育んでいた

- Scalability (早くたくさん決められる合意形成が良いよね)
- Finality (絶対に覆らない合意形成が良いよね)
- Energy efficiency (資源の浪費が少ない合意形成が良いよね)

また、ピアたちの投票力を決める要因についても様々な規範が提案されている

- ストレージの量 (分散型ファイルストレージ, e.g., Filecoin, Arweave, Sia)
- 計算資源量 + トークンの保有量 + トークンの使用量 (Proof of Importance in NEM)
- トークンの保有量<sup>{1/2}</sup> (Quadratic Voting: QV)

# お疲れ様でした！

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
3. 分散性のための合意形成を設計する
  - どのように戦略的行動に対処するか？
  - どのようにスパム・シビル攻撃に対処するか？
  - どのようにただ乗り問題に対処するか？
  - 他の規範にはどのようなものがあるか？
4. 自律性のためのトークン価値を設計する
5. ケーススタディ
6. まとめ



## 4. 自律性のためのトークン価値を設計する

---

価値が付くトークンには何が求められるか？





## どのように市場価値を担保するか(供給側)？

経済学的には "追加1単位供給することにどのくらいコストがかかるか" (限界費用) が重要である

- 売り手としてはそのコストより高く売らないと利益が出ない
- これと需要側の事情 (限界効用に基づく) が一致するところで価格が決まる

### ブロックチェーンの文脈ではどのように担保しているのか？

- Bitcoin protocol: bitcoinの新規発行に費やしたマイニングの計算資源が限界費用
  - 限界費用は難易度調整によって安定化する
  - 限界費用は半減期によって4年ごとに2倍になる (片面だけ見ればどんどん価格が上がる)
- Ethereum: stakingの機会費用が限界費用
  - バリデータになるための32etherを使って色々できたのに、その機会を失っている
  - 裏を返せばstETHなどの仕組みは、etherの価値を毀損することに繋がるのではと (個人的には) 思う

## コラム: Bitcoinの価値の源泉はPoWの電気代なのか？

---

これは PoW vs PoS の文脈などで定期的に話題になる

e.g., etherには価値の裏付けが存在しないからダメだ

しかしこの議論は19世紀の費用価値説 vs 効用価値説の議論を繰り返しているように思う

「価値の源泉が費用なのか効用なのかを議論することは、ハサミの上の刃と下の刃のどちらで紙を切っているのかを議論するようなものである」

要するに議論自体がナンセンス

しかし自分が知る限り、こうした指摘をする人はほとんど存在しない（経済学を勉強した人ならば絶対に知っているはずの話なのに！）

経済学とブロックチェーンの間にまだまだ断絶があることを示す例なのではないかと思う

## どのように市場価値を担保するか(供給側)？

### ブロックチェーンの文脈ではどのように担保しているのか？ (つづき)

- Initial Coin Offering (ICO): 販売トークン1単位を得るために必要な他のトークン (多くはether) が限界費用
- Lockdrops: 販売トークン1単位を得るためにstakeした他のトークン (多くはether) の機会費用が限界費用
  - 一定期間トークン (多くはether) をロックすると販売トークンが貰える
  - 基本的にロックしている期間が長いほど販売トークンがたくさん貰える

### 経済学の文脈ではどのように議論しているのか？

- 基本的には設計よりもvaluationの研究が多い (恐らく価値の議論にはすでに決着が付いているから)
- Bitcoin Protocol: Hayes (2015, 2017, 2019) による cost-of-production model
  - マイニングに費やした計算資源は定量的に把握可能なので、それを元にbitcoinのvaluationを行う
- Ethereum: Fanti et al. (2019) によるvaluation
  - PoSの機会費用を「金融市場における同程度のリスクに対する期待リターン」で推定した

## どのように市場価値を担保するか(需要側)?

経済学的には "追加1単位需要することでどのくらい満足度が得られるか" (限界効用) が重要である

- 買い手としてはその満足度より安く買えるならばどんどん買うはず
- これと供給側の事情 (限界費用に基づく) が一致するところで価格が決まる

### ブロックチェーンの文脈ではどのように担保しているのか?

- Bitcoin protocol: "Peer-to-peer electronic cash system"として, トランザクション手数料としての限界効用
  - おそらく利用が増えるほどに限界効用は指数関数的に増加する
- Ethereum: DAppsを動かすための燃料としての限界効用
  - Bitcoinが digital-gold とたえられるのに対して etherが digital-oil とたえられる所以

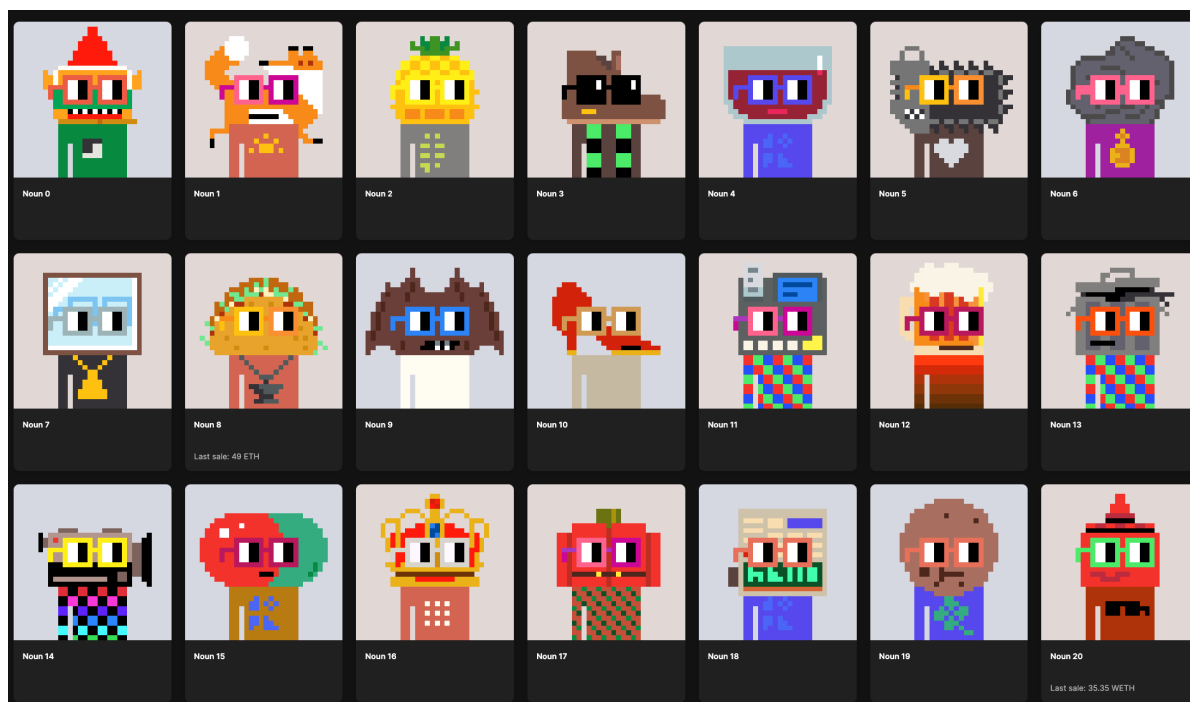
DAppsは他にも様々な限界効用を設計してきた

- 株式とのアナロジー: トークン保有者はガバナンスへの参加や利益の分配から効用を得る
  - DAOのガバナンストークン
  - Decentralized Exchange (DEX) のガバナンストークン, Liquidity Provider (LP)トークン (後述)
- アートとのアナロジー: トークン保有者はトークンのデザインやレアリティから効用を得る
  - NFT (Cryptokitties, Cryptopunks)

## どのように市場価値を担保するか(需要側)?

### ブロックチェーンの文脈ではどのように担保しているのか? (つづき)

- 両者は組み合わさっている場合もある (e.g., Nouns DAO)
  - 1日に1つNFTが新規発行され、このNFTがDAOのガバナンストークンにもなっている (詳細は後述)



## どのように市場価値を担保するか(需要側)?

### 経済学の文脈ではどのように議論しているのか?

- 基本的には設計よりもvaluationの研究が多い (恐らく価値の議論にはすでに決着が付いているから)
  - 限界効用をどのように定量化するのか?
- Bitcoin Protocol:
  - アドレスの数やノードの数 (で推定する送金ネットワークの大きさ) が一般的な代理指標
- より一般的なトークン:
  - 現在のユーザー数とトランザクション数から現在および将来のトークンの価値を推定 (Cong et al. 2021)
  - 一定期間に総供給量の内どの程度が動いているか?, 総供給量の内どの程度がstakeされているか?, 総供給量が毎年どのくらいのペースで増えるか? からトークンの価値を推定 (Liu 2022)
- 定期的に報酬が発生するトークン (e.g., LPトークン)
  - 伝統的な株式のvaluationモデル (e.g., DCF法) を応用する
- NFT
  - 保有アドレス数やトランザクション数に加えて、視覚的なイメージやテキスト説明を用いる研究も存在

## どのように市場価格を安定化するか？

トークンをインセンティブとして活用する場合、価格が付くことに加えてその価格が激しく変動しないことが重要である

### ブロックチェーンの文脈ではどのように担保しているのか？

- 主にプロトコル層でスタビライザー的な機能が実装されている
- Bitcoin protocol: 難易度調整
  - 本来の目的は block-intervalを出来るだけ一定に保つことである
  - しかし限界費用の激しい変動を抑える、限界費用を予測しやすくする、という側面もあるだろう
- Bitcoin protocol, Ethereum: トランザクション手数料
  - オークション型 (送金者が任意の値を入力して高い順にブロックに格納される) の手数料を採用
  - Ethereumはオークション型とブロック規定型の2階建て
  - いずれもネットワークの混雑を平準化することが目的である
  - しかし限界効用の激しい変動を抑える、限界効用を予測しやすくする、という側面もあるだろう





# どのように市場価格を安定化するか？

## 経済学の文脈ではどのように議論しているのか？

- こうしたスタビライザー的機能の分析と改善提案が行われている
- 難易度調整
  - 2016ブロック毎ではなくブロック毎に行ったほうが良い (Noda et al. 2020)
  - 反対にblock-intervalが所与のしきい値を超えた場合にのみ行ったほうが良い (Saito and Iwamura 2019)
- トランザクション手数料 (オークション理論を用いた研究が多い)
  - 手数料は送金者が申告した値の次に高い申告値分を徴収した方が良い (i.e., second price auction)
  - 手数料はブロック内のトランザクションから同じ金額を徴収した方が良い (i.e., monopolistic auction)
- Ethereumの手数料は、base feeは前のブロックと入札を、priority feeはsecond price auctionを採用した方が良い (Chung and Shi 2023)



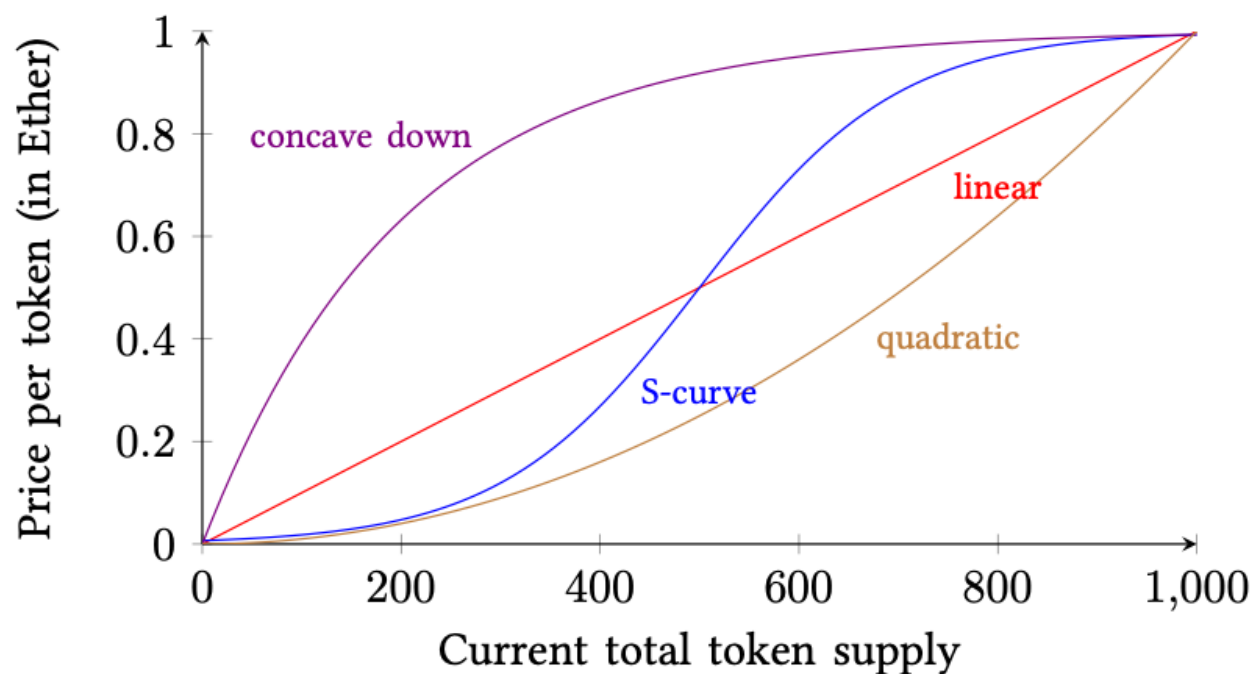
## どのように市場価格を安定化するか(ペッグ)?

安定化に関するより直接的な方法は、トークンと別の資産の交換比率を事前に定義することである

### ブロックチェーンの文脈ではどのように担保しているのか?

- 主にアプリケーション層でいくつかの設計が成されている
- Stablecoin: 別の資産とペッグしてしまう
  - 資産担保型 (e.g., USDT, PAX Gold): ペッグ対象の資産を発行主体 (カストディアン) が保有している
    - 集権的
  - クリプト担保型 (e.g., DAI stablecoin): たとえばetherを担保にUSDペッグのStablecoinを発行する
    - 誰でもカストディアンになれるのでより分散的
    - しかしペッグを維持するためにovercollateralizationが求められる
  - アルゴリズム型 (e.g., Basis, TerraUSD): 担保が存在せず、なんらかのアルゴリズムでペッグを維持する
    - 様々な提案が成されている
    - しかしまだ実用的なものは存在しない (後述)
- もう1つのアプローチは「交換比率自体ではなく、交換比率のルールを事前に定義」すること
  - Token Bonding Curve (TBC)
  - Automated Market Maker (AMM)

## どのように市場価格を安定化するか(ペッグ)?



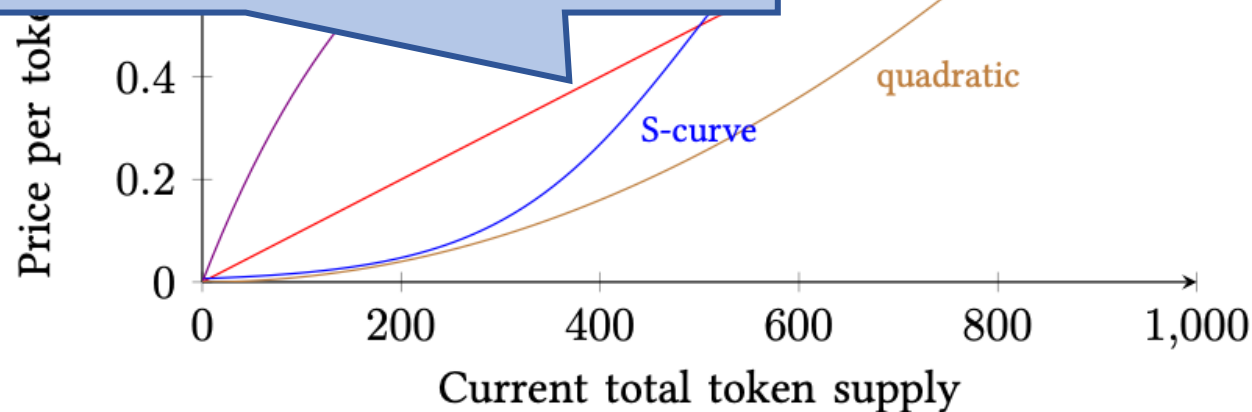
TBC / Etherを預けるとトークンが返ってくる (and vice versa) コントラクト / 交換比率はトークン供給量に応じて決まる

## どのように市場価格を安定化するか(ペッグ)?

最初にトークンを手に入れその後トークン供給量が増えたらetherに戻す、  
という形でetherを増やすことが可能(交換比率が右上がりならば)

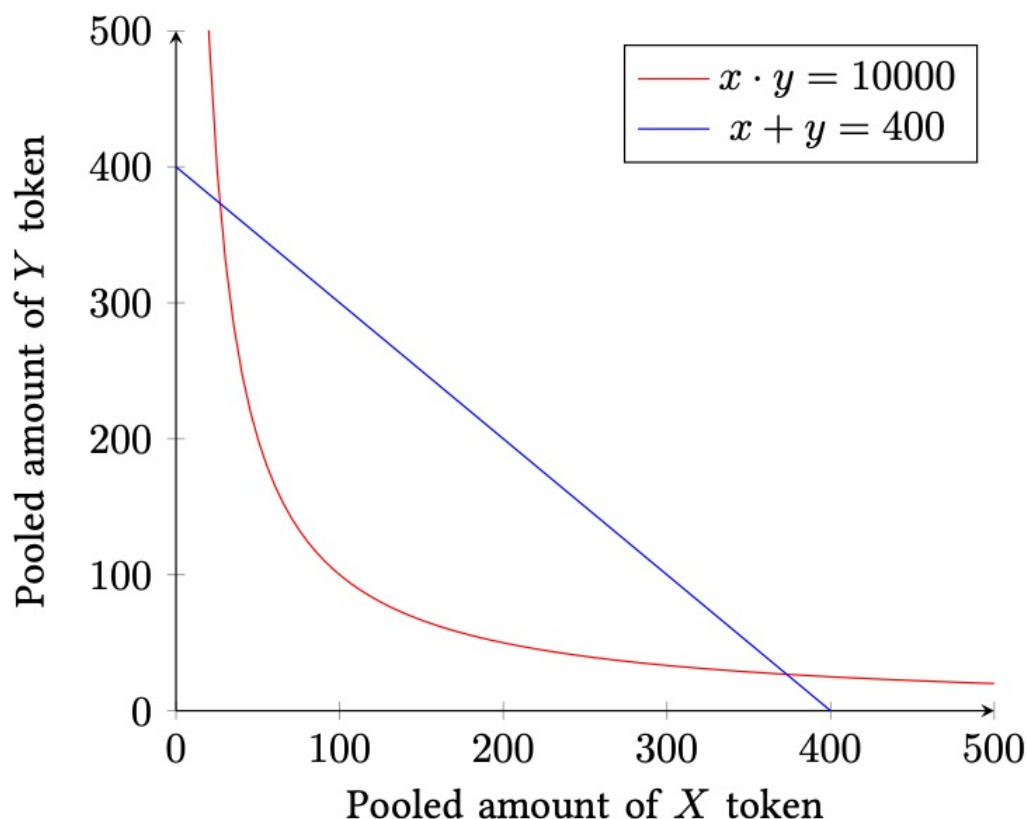
アーティストのNFT販売などに使えるかもしれない

自律的にトークン価格(ether建て)が決まる



TBC / Etherを預けるとトークンが返ってくる (and vice versa) コントラクト / 交換比率はトークン供給量に応じて決まる

## どのように市場価格を安定化するか(ペッグ)?



### Automated Market Maker (a simple example)

#### Create a liquidity pool:

- Peers can create a liquidity pool comprising two types of tokens,  $X$  and  $Y$ .
- A liquidity pool is established when it satisfies the formula:

$$x \cdot y = k,$$

where  $x$  and  $y$  denote the pooled amounts of  $X$  and  $Y$ , respectively, and  $k$  is a constant value.

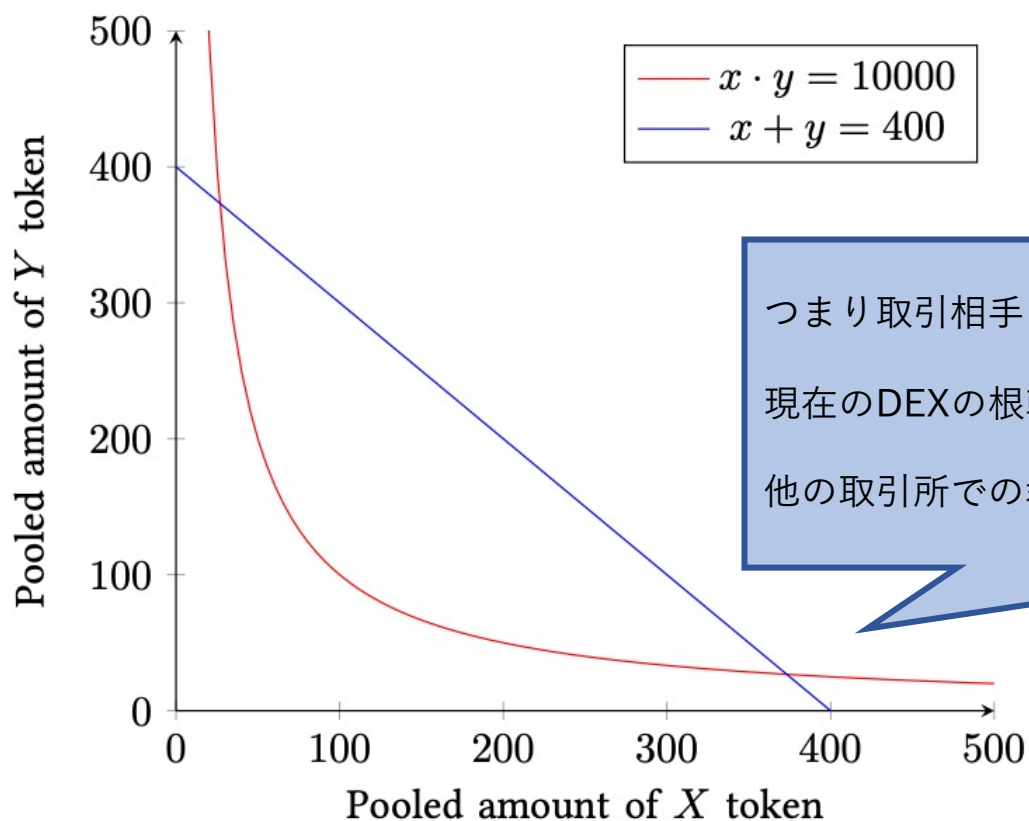
#### Exchange tokens in the liquidity pool:

- Peers can exchange  $X$  and  $Y$  through the liquidity pool.
- The exchange ratio maintains the formula above; exchanging  $\Delta x$  of  $X$  for  $Y$  yields  $\Delta y$  such that  $(x + \Delta x)(y - \Delta y) = k$ .<sup>a</sup>

<sup>a</sup>Exchange fees are omitted for simplicity.

AMM / TBCを2種類のトークンに拡張したコントラクト / 交換比率はpool内のトークン量に応じて決まる

# どのように市場価格を安定化するか(ペッグ)?



## Automated Market Maker (a simple example)

Create a liquidity pool:

- Peers can create a liquidity pool comprising two types of tokens, X and Y.
- A liquidity pool is established when it satisfies

つまり取引相手を見つけずとも、いつでもトークンの交換が行える！

現在のDEXの根幹設計

他の取引所での裁定取引を通じて、自律的にトークン価格が決まる

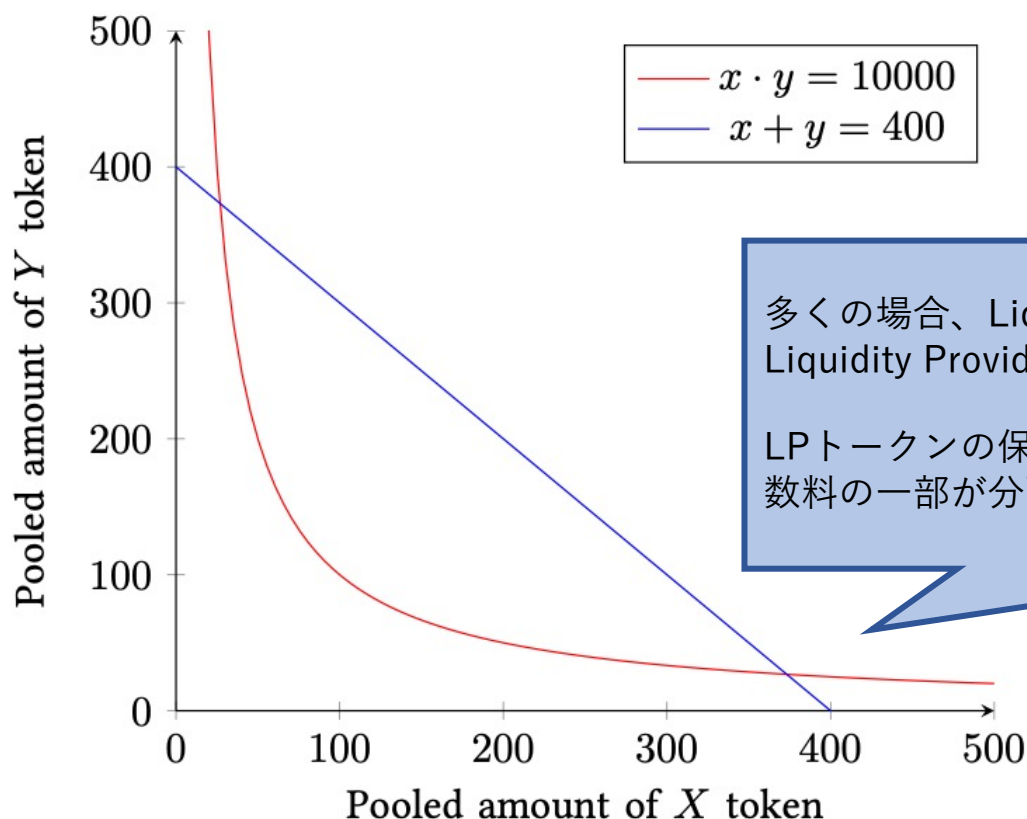
liquidity pool.

- The exchange ratio maintains the formula above; exchanging  $\Delta x$  of X for Y yields  $\Delta y$  such that  $(x + \Delta x)(y - \Delta y) = k$ .<sup>a</sup>

<sup>a</sup>Exchange fees are omitted for simplicity.

AMM / TBCを2種類のトークンに拡張したコントラクト / 交換比率はpool内のトークン量に応じて決まる

# どのように市場価格を安定化するか(ペッグ)?



## Automated Market Maker (a simple example)

Create a liquidity pool:

- Peers can create a liquidity pool comprising two types of tokens, X and Y.
- A liquidity pool is established when it satisfies

多くの場合、Liquidity poolにトークンを提供したEOAに対しては Liquidity Provider (LP) トークンが付与される

LPトークンの所有者には、AMMでトークンを交換する際に徴収される手数料の一部が分配される

liquidity pool.

- The exchange ratio maintains the formula above; exchanging  $\Delta x$  of X for Y yields  $\Delta y$  such that  $(x + \Delta x)(y - \Delta y) = k$ .<sup>a</sup>

<sup>a</sup>Exchange fees are omitted for simplicity.

AMM / TBCを2種類のトークンに拡張したコントラクト / 交換比率はpool内のトークン量に応じて決まる



# どのように市場価格を安定化するか(ペッグ)?

## 経済学の文脈ではどのように議論しているのか?

- Stablecoin: 期待に関する動学的な研究を応用する
  - 資産担保型, クリプト担保型: 通貨危機や銀行の取り付け騒ぎのモデルを応用して頑健性を分析
  - アルゴリズム型: Basisの失敗を元に、ポンジスキームのモデルを元にアルゴリズム型の失敗を分析
- TBC, AMM
  - 定式化が中心で、モデルの提案は少ない
    - 伊東が知る限りでは Krishnamachari et al. (2021) がAMMの  $k$  を変動性にするという提案をしている
    - DEX運営組織など、実務家の方がTBC, AMMの設計は進んでいる
  - しかし個人的には、経済学が貢献できる部分はまだまだあると思う
    - AMMは経済学における無差別曲線と同じ構造だから
    - こういう提案を経済学の側が出せなかったことが悔しい



# お疲れ様でした！

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
3. 分散性のための合意形成を設計する
4. 自律性のためのトークン価値を設計する
  - どのように市場価値を担保するか (供給側) ?
  - どのように市場価値を担保するか (需要側) ?
  - どのように市場価格を安定化するか ?
  - どのように市場価格を安定化するか (ペッグ) ?
5. ケーススタディ
6. まとめ





## 5. ケーススタディ

---

各要素をどこまで同時に達成しているのか？

	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

# Bitcoin Protocol

"Peer-to-peer electronic cash system"のためにインセンティブを活用した最初の実用的なプロトコル

- 戦略的行動: PoWとNakamoto consensusの組み合わせで対処
- スпам・シビル攻撃: トランザクション手数料とPoWでそれぞれ対処
- ただ乗り問題: Nakamoto consensusとCoinbaseの組み合わせで対処
- 限界費用: PoWとCoinbaseの組み合わせで担保 (半減期で経時的に上昇)
- 限界効用: Peer-to-peer electronic cash systemとして担保
- 安定化: 難易度調整

## 伊東の解釈・評価

上手く出来ている、1つの機能に複数の役割・意味合いが込められていることがわかる

自律分散的な仕組みを設計する上でのベンチマークたりうる

他の規範 (e.g., scalability, finality, energy efficiency) やガバナンスがさらなる検討要素だろう



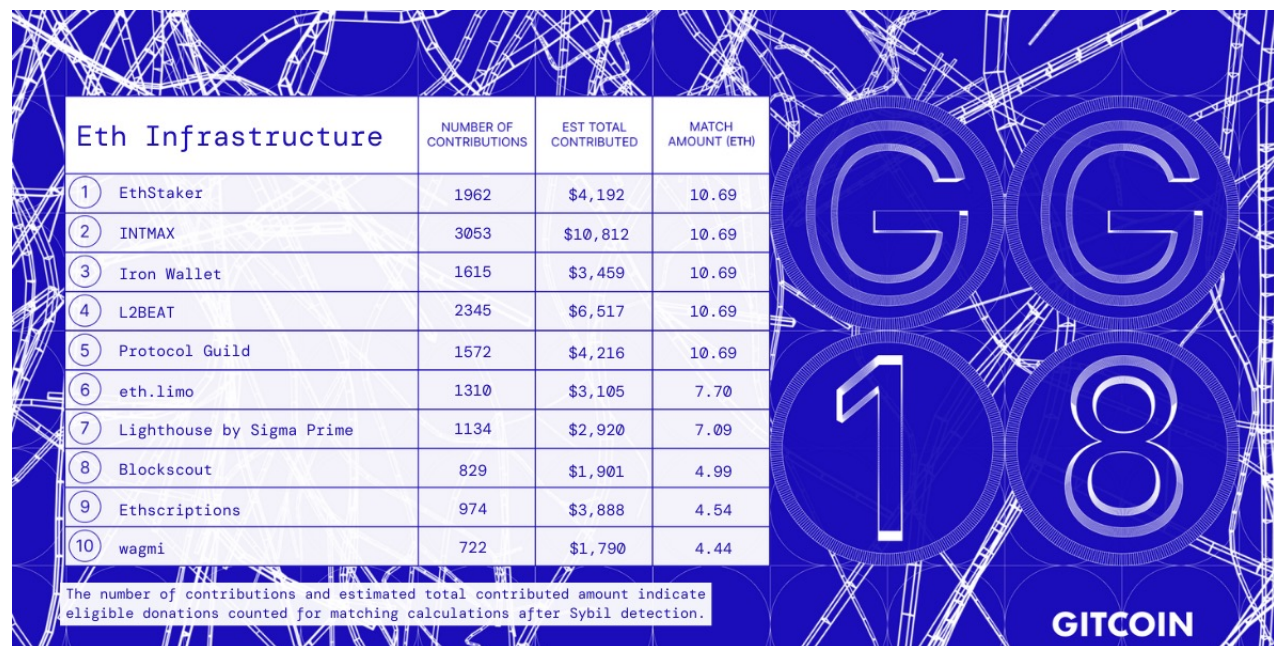
	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

# Gitcoin

Ethereum上のDAppsであり、オープンソースプロジェクトへの寄付プラットフォーム

- 利用者は任意量のether (またはstablecoin) をGitcoinにpoolすることができる
- プールされたetherは、リストされているオープンソースプロジェクトに配分される
  - どのプロジェクトをリストするかは集権的な運営が決めている
  - 一方で、poolしたetherを各プロジェクトにどれだけ配分するか？はQVの応用で決めている

\* QVに用いたetherはそのままプロジェクトに寄付され、poolからの拠出額をQVの重み付けで決めている



Eth Infrastructure		NUMBER OF CONTRIBUTIONS	EST TOTAL CONTRIBUTED	MATCH AMOUNT (ETH)
1	EthStaker	1962	\$4,192	10.69
2	INTMAX	3053	\$10,812	10.69
3	Iron Wallet	1615	\$3,459	10.69
4	L2BEAT	2345	\$6,517	10.69
5	Protocol Guild	1572	\$4,216	10.69
6	eth.limo	1310	\$3,105	7.70
7	Lighthouse by Sigma Prime	1134	\$2,920	7.09
8	Blockscout	829	\$1,901	4.99
9	Ethscriptions	974	\$3,888	4.54
10	wagmi	722	\$1,790	4.44

The number of contributions and estimated total contributed amount indicate eligible donations counted for matching calculations after Sybil detection.

**GITCOIN**



# Bitcoin

- 戦略的行動: QVはシビル攻撃に脆弱, たとえ1人1アカウントが担保できても談合 (collusion) に脆弱
- スпам・シビル攻撃: 集権的に対処 (Bitcoin Passport; 利用者にSNSアカウントを提出させる)
- ただ乗り問題: 寄付のプラットフォームなのでそもそも不要

また、Bitcoinは2021年にDAO化を目指してBitcoin token (BCT) を発行した

- 限界費用: すべてプレメイン形式なので (恐らく) 無い
- 限界効用: stakeすることでBitcoin Passportのidentity scoreを高められる, ガバナンストークンとしての機能は現在開発中 (らしい)
- 安定化: なし

## 伊東の解釈・評価

QVという新しい規範を実装するために、分散性をある程度犠牲にしている

BCTを通じてQVと自律分散性が両立できれば良いのだろうが、現状はまだその水準には達していない



	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

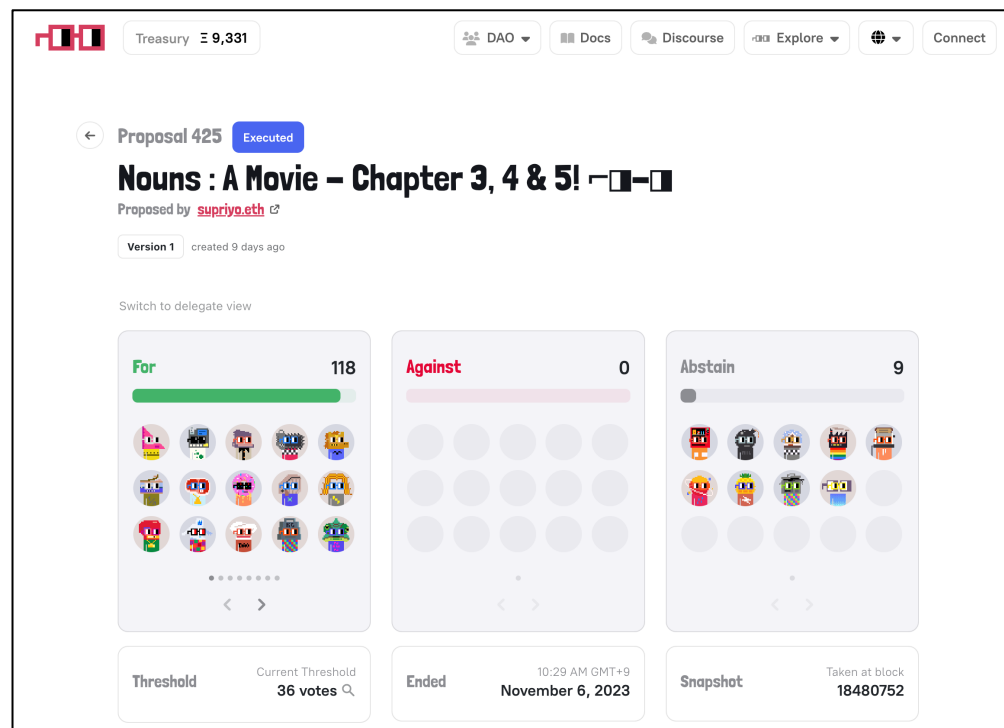


# Nouns DAO

## Ethereum上のDApps

1. Nouns DAOは1日1回 "Noun" と呼ばれるNFTを自動的に発行する
2. Nounは、etherで入札可能なデイリーオークションに出品される (落札者が支払ったetherはpoolされる)
3. Nounの保有者は、poolされたetherを (Noun有名にするために) どう使うか決める投票に参加することができる

\* 投票はtoken-staking方式だが、Nounの再配分は (報酬もペナルティも) ない。あくまで1Noun1票で三択 (for, against, abstain) に投票するだけ



# Nouns DAO

戦略的行動: Token-stakingにより対処

スパム・シビル攻撃: Token-stakingにより対処

ただ乗り問題: (投票で報酬が発生するわけではないので) 対処していない

\* コミュニティの熱が投票の動機になっている状態

限界費用: デイリーオークションの落札額 (ether)

限界効用: アートとして + ガバナンストークンとして

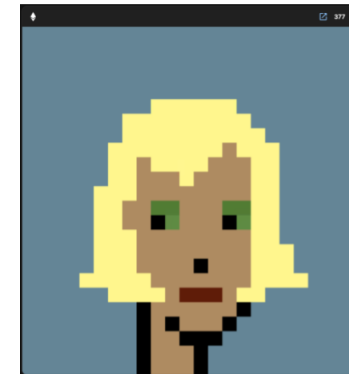
安定化: なし

## 伊東の解釈・評価

良く出来ている、しかしただ乗り問題と価値安定化の仕組みが欠けている

NFTならではの仕組みで改善できないだろうか？

- 投票に使ったNounの特徴を以降発生しにくくする (レアにする) ことで投票参加のインセンティブになる？
- オークションの頻度を過去の平均落札額に応じて変動させる (難易度調整のように) ことで安定化になる？



Traits		
ACCESSORY 3 Attributes 45% Floor: --	ACCESSORY Blonde Bob 1% Floor: --	ACCESSORY Earring 25% Floor: --
ACCESSORY Green Eye Shadow 3% Floor: --	TYPE Female 38% Floor: --	

\* CryptoPunksにはレアリティの概念がある

	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

# Terra

## アルゴリズム型stablecoinを目指したプロトコル

- 2種類のトークンから構成されている: TerraUSD (UST), LUNA

\* 本当は他の法定通貨とペッグしたトークンも存在するが、便宜上割愛

- 前者はstablecoin, 後者はUSTのトランザクション記録の合意形成に参加した報酬 (coinbase)
- USTは1ドル分のLUNAとの交換が約束されており、これがUSTのペッグになっている
- $1\text{UST} < 1\text{USD}$  のとき → USTをLUNAに交換することで利益が出る (裁定取引) → このときLUNAに交換されたUSTはburnされる → USTの総供給量が減る → USTの価値が高まる (and vice versa)

\* 逆の場合はLUNAがburnされるが、このときは全部ではなく一部がburnされる

- プロトコルの合意形成は、PoS (LUNA), Nakamoto consensus, coinbase (LUNA) が活用されている

戦略的行動: PoSとNakamotoコンセンサスの組み合わせにより対処

スパム・シビル攻撃: トランザクション手数料とPoSでそれぞれ対処

ただ乗り問題: PoSとNakamotoコンセンサスの組み合わせにより対処



# Terra

LUNAのトークン価値については以下のとおり

限界費用: なし (LUNAはUSTの交換およびPoSの合意形成で自動的に新規発行される)

限界効用: LUNAのstakingで、トランザクション手数料 (UST) と coinbase (LUNA) を獲得できる

安定化: UST-LUNAの交換以外にも、coinbase (LUNA) や LUNAのburnレートなどに安定化機構が存在

## 伊東の解釈・評価

Bitcoin Protocolを参考にしており、一見すると良く出来ている

しかし2022年にTerraは $1\text{UST} = 1\text{USD}$ のペッグが維持できずに失敗してしまった

- $1\text{UST} < 1\text{USD}$  になる  $\rightarrow$  LUNAに交換しようという需要が高まる  $\rightarrow$  LUNAが新規発行される  $\rightarrow$  LUNAの価格が下がる  $\rightarrow$   $1\text{UST}$ を $1\text{USD}$ 相当のLUNAと交換することが難しくなる  $\rightarrow$  UST価格が下がる  $\rightarrow$  負のスパイラル...

この事件については、参加者の期待に着目した実証研究がいくつか存在する (e.g., Uhlig 2022, Briola et al. 2023)

しかし設計の観点でいえば、ペッグに用いられるLUNAに限界費用が存在しないこと (staking自体が用途という同語反復的な構造) が根本的な原因だと思う

# Terra

LUNAのトークン価値については以下のとおり

限界費用: なし (LUNAはUSTの交換およびPoSの合意形成で自動的に新規発行される)

限界効用: LUNAのstakingで、トランザクション手数料 (UST) と coinbase (LUNA) を獲得できる

安定化: UST-LUNAの交換レートに

先述のとおり、通常stakingはそのトークンが使えなくなるため機会費用が発生し、それが限界費用といえる  
しかしLUNAの場合は用途自体がstakingなので、機会費用が発生していない

## 伊東の解釈・評価

Bitcoin Protocolを参考にしてお

しかし2022年にTerraは1UST = 1USDのpegが維持できずに大暴落してしまった

- 1UST < 1USD になる → LUNAに交換しようという需要が高まる → LUNAが新規発行される → LUNAの価格が下がる → 1USTを1USD相当のLUNAと交換することが難しくなる → UST価格が下がる → 負のスパイラル...

この事件については、参加者の期待に着目した実証研究がいくつか存在する (e.g., Uhlig 2022, Briola et al. 2023)

しかし設計の観点でいえば、ペッグに用いられるLUNAに限界費用が存在しないこと (staking自体が用途という同語反復的な構造) が根本的な原因だと思う

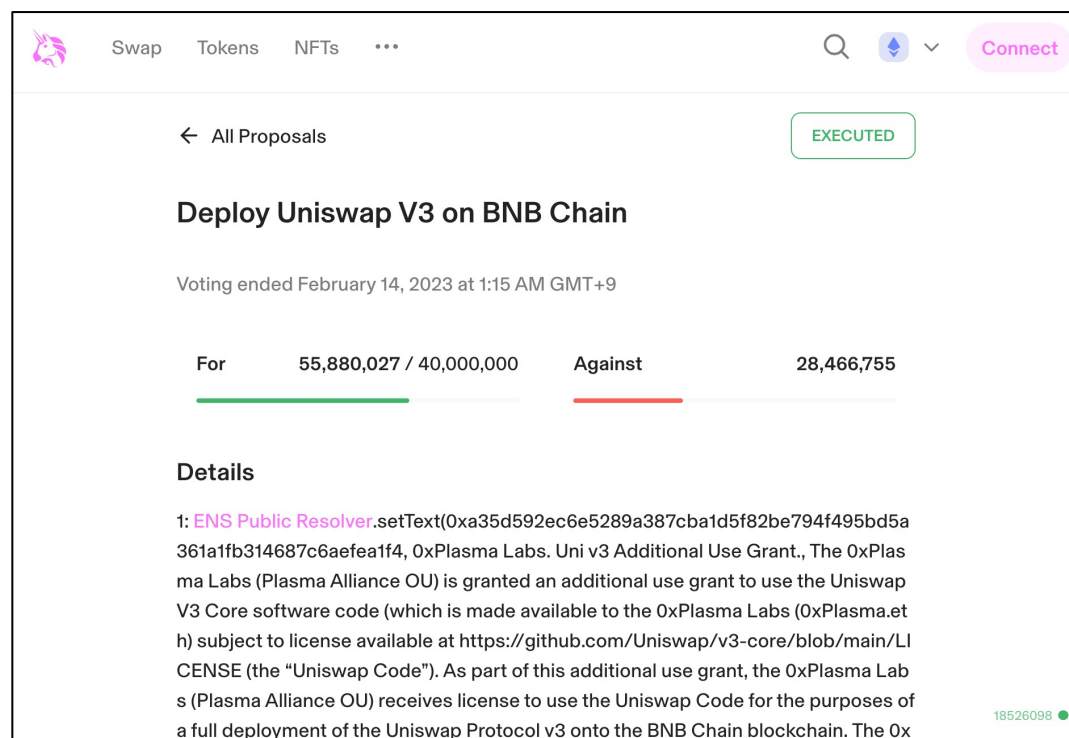
	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

# Uniswap

## Ethereum上のDAppsであり、代表的なDEX

- 2020年にガバナンストークンであるUNIを、liquidity providerを含む複数のEOAに配布した
- 先述のAMMとは別に、ここではUNIについて考える

\* 投票はtoken-staking方式だが、UNIの再配分は（報酬もペナルティも）ない。あくまで1UNI1票で二択（for, against）に投票するだけ





# Uniswap

戦略的行動: Token-stakingにより対処

スパム・シビル攻撃: Token-stakingにより対処

ただ乗り問題: (投票で報酬が発生するわけではないので) 対処していない

\* いくつかの研究 (e.g., Barbereau et al. 2022, Barbereau et al. 2023) がUniswapにおける低い投票率を指摘している

限界費用: liquidity providingの機会費用 - LPトークンから得られる報酬

限界効用: ガバナンストークンとして

安定化: なし

## 伊東の解釈・評価

AMMの仕組みは大変美しい一方で、UNIにはただ乗り問題が残るし限界費用・限界効用ともに弱い

AMMを利用した手数料をLPトークンの保有者だけでなくUNIトークンの保有者にも分配すると限界効用が高まるだろう (fee switchという名前でUniswap内でも議論されている)

しかしそもそもLPトークンをガバナンストークンにすれば良いのでないか？UNIトークンの存在意義は個人的には良くわからない

## コラム: どのような経緯でUNIトークンが生まれたか？

- Uniswapは2018年に実装されており、最初はUNIトークンは存在しなかった
- 2020年に、UniswapのコピープロジェクトであるSushiswapが登場した
- Sushiswapは**Liquidity provider**にガバナンストークン**SUSHI**を配布するというインセンティブ施策をうつことで、UniswapのLiquidity poolから多くのトークンを奪うことに成功した (**Vampire attack**)
- これに対抗すべく、Uniswapも (存在意義が不明瞭な) ガバナンストークンUNIを配布することになった
- 詳細はFan et al. (2023) などを参照のこと



	分散性のための合意形成を設計する			自律性のためのトークン価値を設計する		
	戦略的行動	スパム・シビル攻撃	ただ乗り問題	限界費用	限界効用	安定化
<b>Bitcoin Protocol</b> 統合のベンチマーク	✓	✓	✓	✓	✓	✓
<b>Gitcoin</b> 分散性を緩めてQVを導入		✓ (集権的)	(そもそも要らない)		✓	
<b>Nouns DAO</b> NFT特有の改善の余地あり	✓	✓		✓	✓	
<b>Terra</b> 限界費用の欠如が失敗を招く	✓	✓	✓		✓	✓ (失敗)
<b>Uniswap</b> 存在意義が不明瞭なトークン	✓	✓		✓ (弱い)	✓ (弱い)	

# お疲れ様でした！

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
3. 分散性のための合意形成を設計する
4. 自律性のためのトークン価値を設計する
5. ケーススタディ
  - Bitcoin Protocol
  - Gitcoin
  - NounsDAO
  - Terra
  - Uniswap
6. まとめ



## 6. まとめ

---

## 講義の要旨

---

- Cryptoeconomics と Tokenomics は統合してこそ新規性がある
- 統合のためには、戦略的行動、スパム、シビル攻撃、ただ乗り問題、限界費用、限界効用、安定化、を同時に考慮する必要がある
- ケーススタディでは、同時に考慮することの難しさを示した
- この講義は（伊東が知る限り）Cryptoeconomics と Tokenomics について、経済学とブロックチェーンの文脈を繋ぐ形で体系的にまとめた初めての講義である



## 今後の課題

---

システム外のインセンティブをどのように考慮するか？

- Bitcoin Protocolでは、プロトコル外の取引所で売りポジションを取ることで（たとえcoinbaseがbitcoinでも）プロトコルを毀損するインセンティブが存在する（Goldfinger attack）
- Ethereumでは、アプリケーション層にあるDEXの発達がブロック内のトランザクションを並び替える新たなインセンティブを生み出した（Maximal Extractable Value; MEV）

人間が合理的であるという暗黙の仮定をどのように緩めるか？

- 行動経済学をブロックチェーン関連の議論に応用する、といった話になってくる？



# お疲れ様でした！

---

1. イントロダクション
2. 用語の歴史とそれに対する伊東の意見
3. 分散性のための合意形成を設計する
4. 自律性のためのトークン価値を設計する
5. ケーススタディ
6. まとめ
  - 講義の要旨
  - 今後の課題

