Governance of the Blockchain

土屋研究会 IS 22春 期末発表

2022/07/06　B2 竹村 太希

研究の背景

ガバナンス問題

- ブロックチェーンはトラストレスと信じられているが...
- 仕様変更などの際, **コア開発者・ノード運営者に権力が集中している**ことが指摘されている
- このままでは安定的なブロックチェーンの運用が達成されない可能性がある
- 適切なガバナンスシステムを用意する必要性が高まっている
- **ブロックチェーンガバナンス**の定義:
  - パブリックブロックチェーンコミュニティと主要なステークホルダーが, 特にプロトコル変更に関して集団行動に至る方法 (Carter 2018)

研究の目的

- ブロックチェーンの適切なガバナンスモデルを模索したい

前回までの調査

ガバナンスにまつわる問題点の事例調査

- いくつかの事例から問題点を調査
  - Bitcoinのブロックサイズ論争
    - Governance of the blockchainの問題が明るみになった事件
  - Ethereum The DAO事件
    - コア開発者とノード運営者が過去の取引をなかったことにしてしまう
    - コミュニティが分裂し, ハードフォークが発生した

前回までの調査

オンチェーンでのガバナンスシステムを調査

- Polkadot
  - ノードのランタイムをチェーン上で管理し，フォークレスアップグレードを実現
  - トークンベースの投票システムを設け，承認されればランタイムを更新できる
  - お金持ち優位な政治では?

最近やったこと

- 前回は事故事例の調査が中心だった
- オフチェーンガバナンスと, オンチェーンガバナンスのメリット・デメリットを整理した
  - オフチェーンガバナンスを採用しているチェーンの例: Bitcoinのガバナンスの仕組みを詳細に調べた
  - オンチェーンガバナンスを採用しているチェーンの例: Polkadot (前回調べた)

Bitcoin

BIP

- BIPとは?
  - **Bitcoin Improvement Proposal**
  - Bitcoinの新機能提案を行う技術的な設計文書
  - GitHubで管理されている
- 例えばどんなものがあるの?
  - BIP-2: BIP process, revised
    BIPについて定めたもの
  - BIP-141: Segregated Witness (Consensus Layer)
    ブロックの構造を変えることにより, スケーリング問題などに対処する

Bitcoin

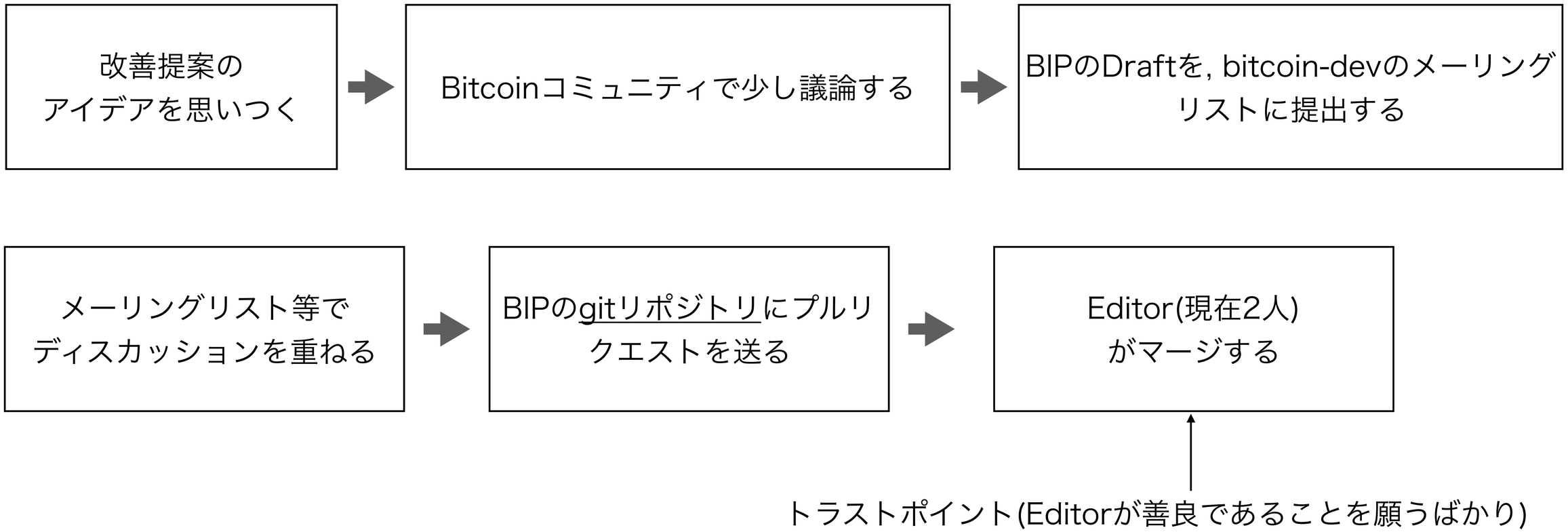
BIP

- BIPの種類
  - **Standard Track BIP** ← BIP-141: Segregated Witness (Consensus Layer)
    プロトコル変更や検証ルールの変更など, インターオペラビリティに影響を与える項目.
    BIP(設計ドキュメント)→参照実装(Bitcoin Core)への取り込み
  - **Informational BIP**
    一般的なガイドラインや情報をコミュニティに提供するもの
  - **Process BIP** ← BIP-2: BIP process, revised
    Bitcoinを取り巻く様々なプロセス(ex: 意思決定プロセス)の変更を提案したりする.
    Informational BIPと異なり, ユーザーは無視することが出来ない.

Bitcoin

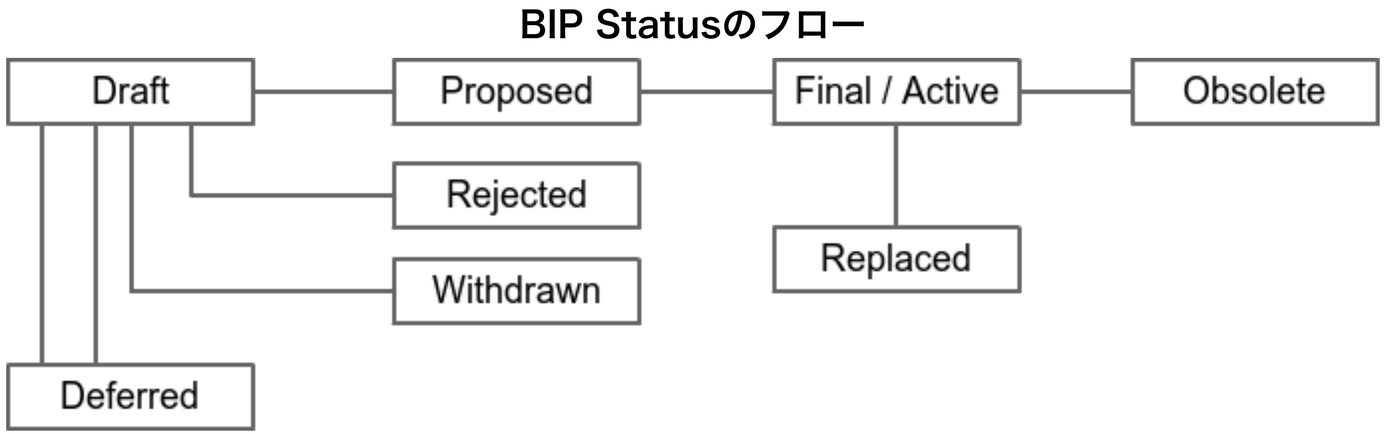
BIP

- BIP反映のプロセス



Bitcoin

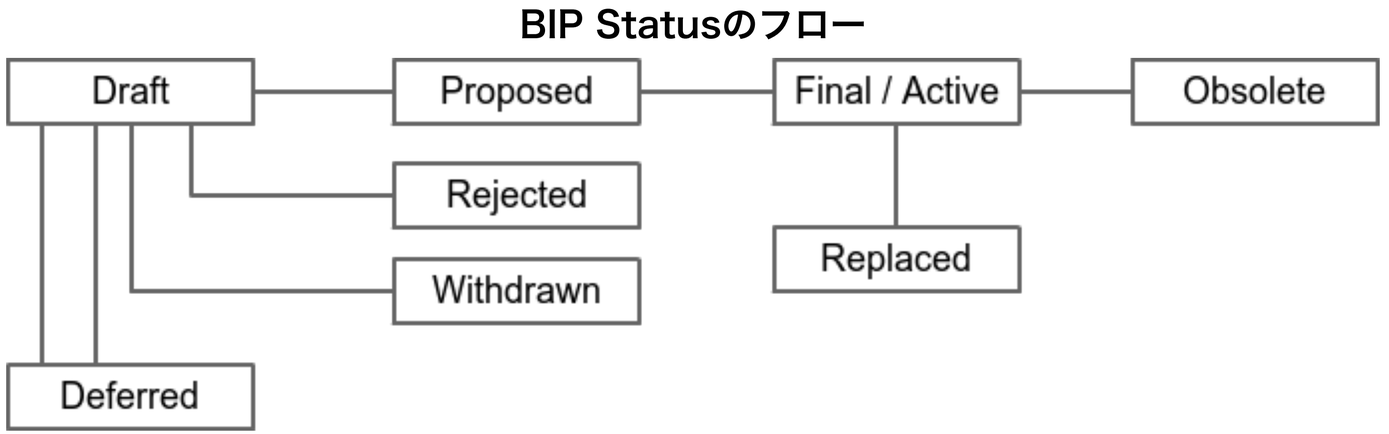
BIP



- BIPの著者:
  - Draft, Deferred, Withdrawnは自分で設定できる
- 有効な実装があり, Finalに進めるためのコミュニティ計画があれば, DraftからProposedにステータスが移行する
- 3年間進捗がなければ, Draft/ProposedからRejectedにステータスが変更される
- ProposedなBIPは, 実世界で採用された場合Finalに変更される(次のスライドで)
- もう適切なBIPではなくなった場合にObsolete/Replacedとなる

Bitcoin

BIP



- Finalステータスへの移行
  - ハードフォーク or ソフトフォーク
    - ハードフォーク: チェーンの分岐を伴う
    - ソフトフォーク: 後方互換性のあるフォーク
      旧ルールの制限をより狭める等
  - ソフトフォークが必要なBIPは, チェーン上の投票によりマイナーの95%の賛成が必要となる (BIP-9で定義されている投票プロセス)

Bitcoin

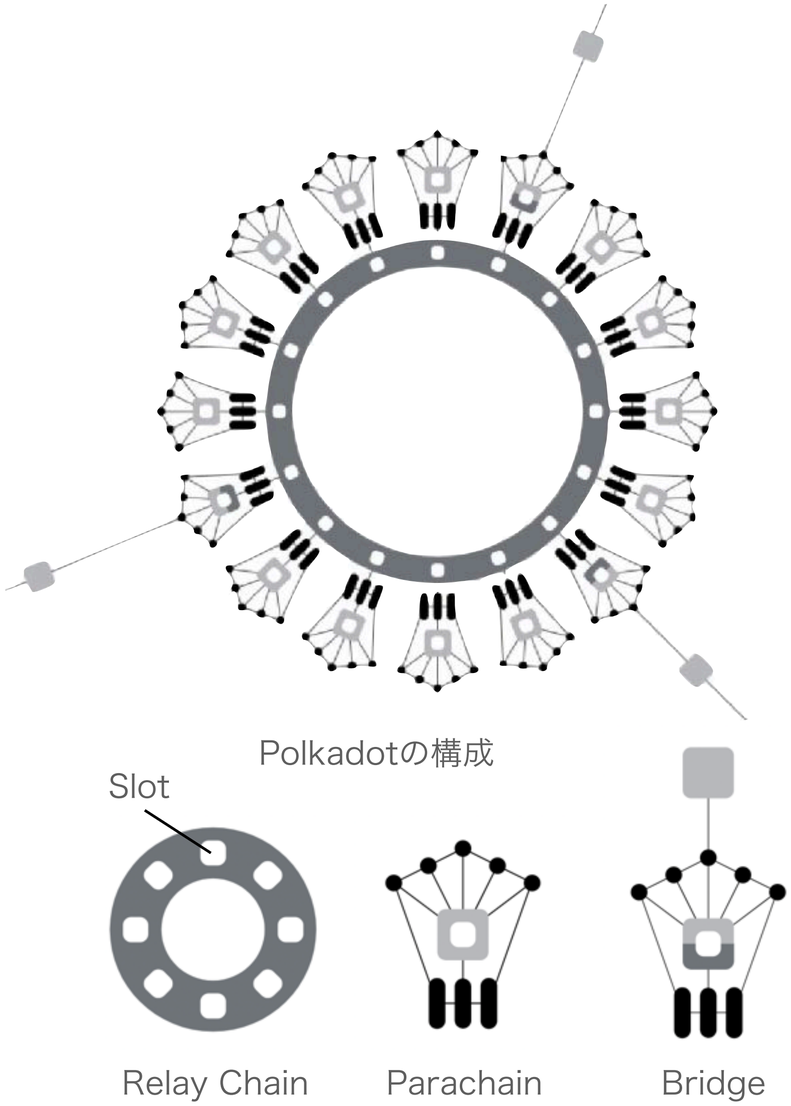
BIP

- Case: Segwit (Segregated Witness)
  - ソフトフォークによって実現
  - なかなかマイナーの賛同を得られなかったので, BIPを乱発して通した

Polkadot

洗練されたガバナンスシステムの例

- 後発のブロックチェーンでは, 暗黙的でないガバナンスシステムを設けているものがある
- Polkadot: 複数のブロックチェーンを繋げることができ, Interoperabilityをもたせるチェーン



Polkadot

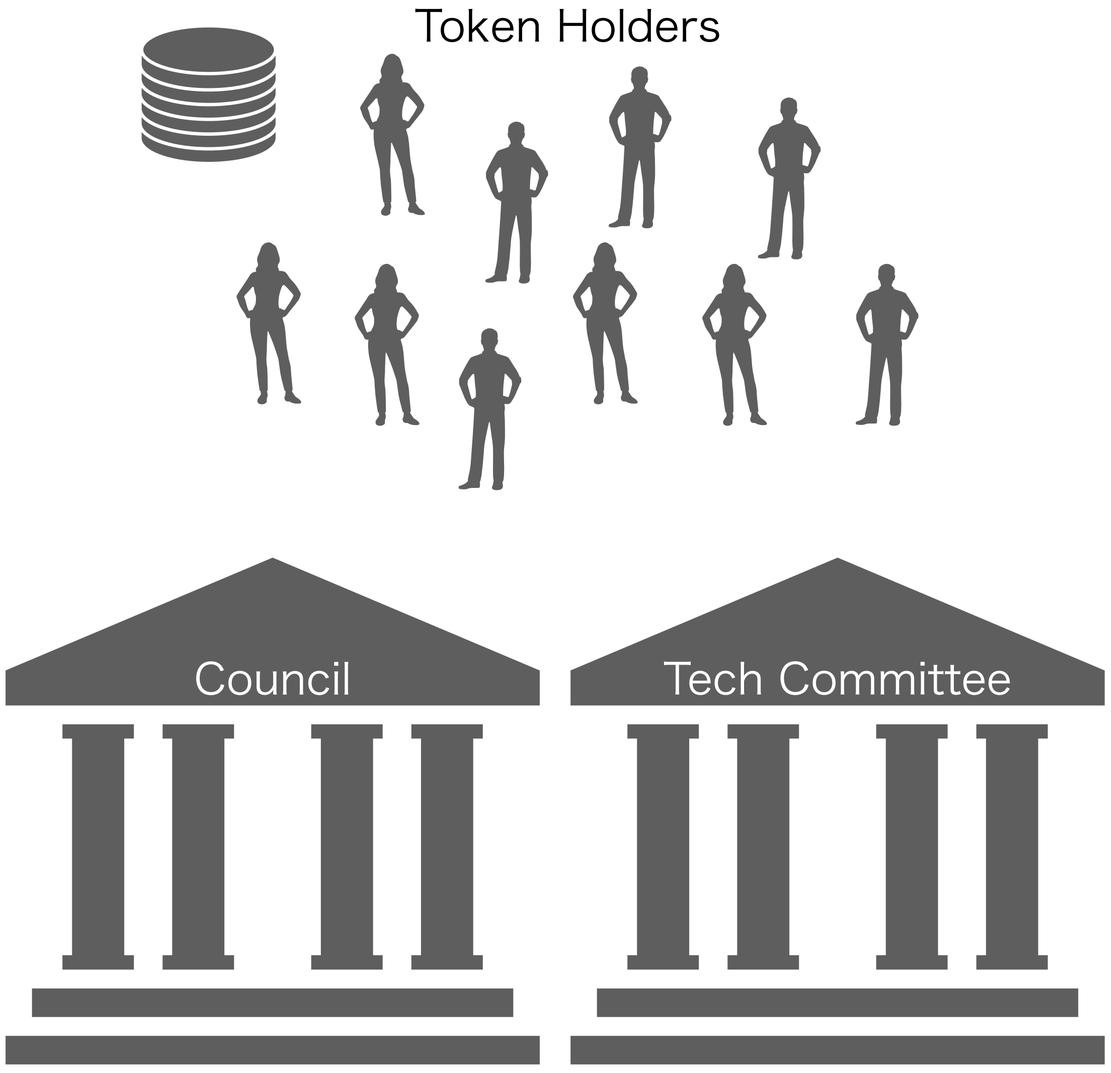
フォークレスアップグレード

- Polkadotノードのランタイムはwasmで書かれており, チェーン自体に保存されている
- チェーン上のランタイムデータを変更すれば, ハードフォークすることなくランタイムを更新できる
- **トークンホルダーを中心に投票を行い, 承認されれば更新される仕組み**

Polkadot

ステークホルダー

- Token holders
- Council Members
  - 投票の提案, 拒否権の発動ができる
  - Token holderから選出される
- Technical Committee
  - コア開発者メンバーで構成
  - 緊急の投票提案ができる



CouncilとTechnical Committeeの二院制

Polkadot

提案の発議

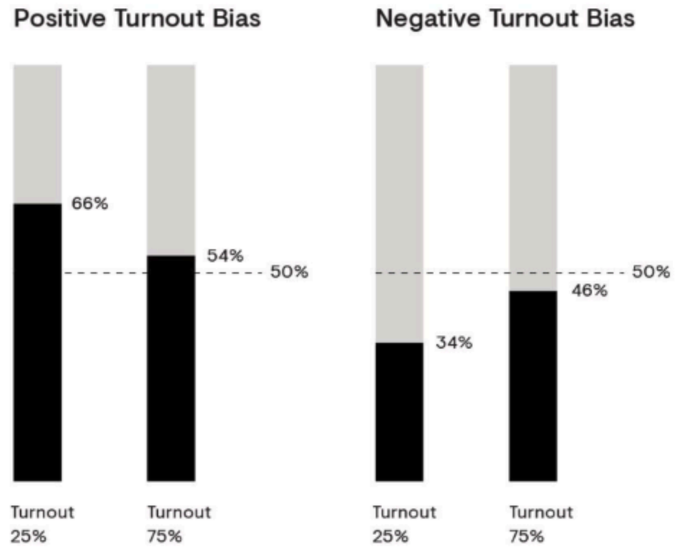
- 提案の種類
  - **Public referenda**
    - 一定の期間トークンを預けることで投票の提案ができる
    - 同額のトークンを預けることで賛成できる
    - 最も賛成を得た提案が, 次の投票プロセスに回される
  - **Council referenda**
    - Council発の議案は即次の投票プロセスに回される

Polkadot

投票

- 投票は28日ごとに行われる
- Token holderは, トークンを預けることで投票ができる
- **Adaptive Quorum Biasing**を採用
  提案に対して大きな反対(賛成)がない場合に可決(否決)を用意にする
  - **Positive Turnout Bias**
    - 投票率が低いときは賛成票の超過半数が必要だが, 投票率が100%に近づくにつれ単純多数決になる
  - **Negative Turnout Bias**
    - 投票率が低いときは反対票の超過半数が必要だが, 投票率が100%に近づくにつれ単純多数決になる

提案形式	成立条件
Public Referenda	Positive Turnout Bias (Super-Majority Approve)
Council Referenda (全会一致)	Negative Turnout Bias (Super-Majority Against)
Council Referenda (過半数の賛成)	単純多数決



Polkadot

問題

- Polkadot以外にも似たようなシステムを採用しているチェーンは複数あるが, **投票にトークンを用いる時点でお金持ち優位**であり, 到底民主的とは呼べないのではないか
- 一方, **ブロックチェーン上で”一人一票”を実現することは難しい**

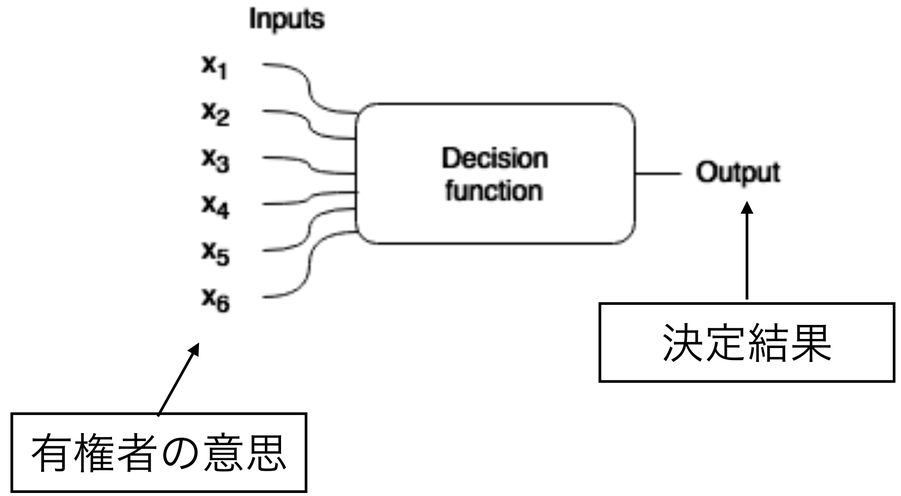
オフチェーンガバナンス vs オンチェーンガバナンス

- BitcoinやEthereumのようなオフチェーン型のガバナンスと, Polkadotのようなオンチェーン型のガバナンスシステムに分類される
- どちらがマシか, 様々な議論が行われていた

オフチェーンガバナンス vs オンチェーンガバナンス

ガバナンス観による違い

- ガバナンスを, 意思決定機能と捉える場合
  - ガバナンスシステムは関数として扱える
  - 決定論的な関数であると嬉しい
  - 計算量が少ないと嬉しい
  - オンチェーンガバナンスに分がある



オフチェーンガバナンス vs オンチェーンガバナンス

ガバナンス観による違い

- ガバナンスを, 調整機関として捉える場合
  - コインホルダーとその他のアクターの利害が対立することは多々ある
  - 様々な声を聞き, 全体のラフコンセンサスを形成し, 協調していく必要がある
  - オフチェーンガバナンスに分がある

オフチェーンガバナンス vs オンチェーンガバナンス

メリットとデメリット

- オンチェーンガバナンスのメリット
  - Verifiableなのでアカウンタビリティの担保が出来る
  - 意思決定に拘束力をもたせることができる
  - ハードフォークの可能性を低く抑えられる
  - 分散型
  - 投票ルールをプログラム可能
- デメリット
  - 低い投票率
  - 金権政治

オフチェーンガバナンス vs オンチェーンガバナンス

メリットとデメリット

- オフチェーンガバナンスのメリット
  - ラフなコンセンサスを形成しやすい. 協調できる可能性がある.
- デメリット
  - メーリングリストやTwitter, Redditなどでバラバラに不定期開催される不透明な議論
  - 議論のプラットフォーム上で, 書き込みを増やして声を大きく見せることが(理論上)可能
  - ハードフォークの可能性が大きい
  - 中央集権的

考察(感想)

マルチステークホルダー型のガバナンスへ

- トークンベースの投票によるオンチェーンガバナンスは金権政治に陥る可能性が高く, 多くの/多様なユーザーの声を反映しているとはいい難い→正統性に疑問が残るのでは?
  - ~~(そもそも, ガバナントークン売って設ける口実だろ…)~~
- とはいえBitcoinのような既存のオフチェーンガバナンスも, 現状, 本当に多様性あふれる集団による議論が行われているのだろうか
  - コア開発者・マイナー(マイニングプール運営者)・ノード運営者の声が大きすぎる
- いい感じのマルチステークホルダーガバナンスやりたい

今後の予定

- 他のチェーンについても調べてみる
  - 最終レポートは, 各チェーンのガバナンスモデルを調べて分類する予定
- マルチステークホルダーモデルでいい感じにできないかなという感想があります
  - コインホルダー, マイナー, ノード運営者, 規制当局, アプリケーション開発者, 先進国の人々, 発展途上国の人々, etc…
  - いい感じ: マルチステークホルダーで(技術的に)拘束力のある決定ができる

参考文献

- “BIP-2"
  https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki
- "BIP-9"
  https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki
- 安土 茂亨 “動画で学ぶブロックチェーン】Bitcoinのソフトフォークのデプロイ方法" (2021)
  https://www.youtube.com/watch?v=_3fgK4aYz3E
- Pierre Rochard "Bitcoin Governance” (2018)
  https://pierre-rochard.medium.com/bitcoin-governance-37e86299470f
- Vitalik Buterin "Notes on Blockchain Governance” (2017)
  https://vitalik.ca/general/2017/12/17/voting.html
- EthHub “Governance on Ethereum”
  https://docs.ethhub.io/ethereum-basics/governance/
- Phil Lucsok “Why on-chain governance?” (2018)
  https://medium.com/polkadot-network/why-on-chain-governance-82ecf28f314c