Governance of the Blockchain

土屋研究会 IS 22春 中間発表

2022/05/25　B2 kekeho

研究概要

- 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

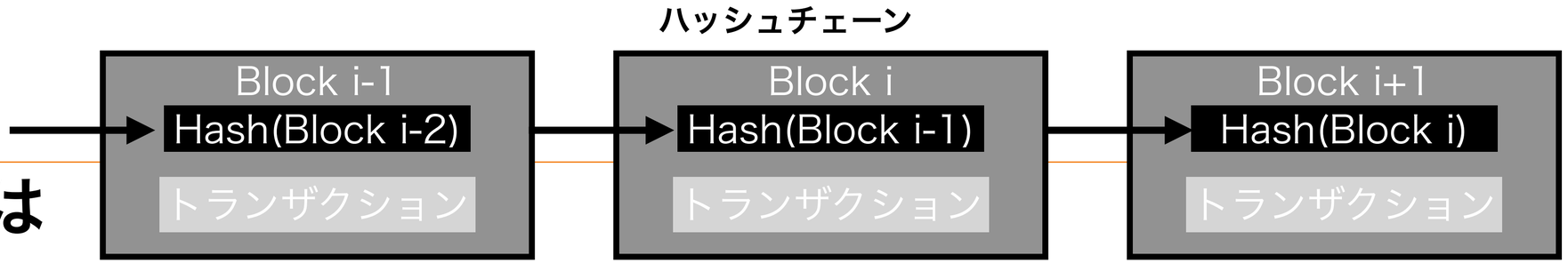
研究の背景

ブロックチェーンを理解するための前提知識

- デジタル署名の要件
  - **完全性**: メッセージの欠損や不整合がないことを保証する
  - **正真性**: メッセージが作成名義人の意思に基づいて作成されていることを証明する
- **ハッシュ関数**: 任意のサイズのデータを入力すると, 一定のビット列のサイズの数値を出力する関数
  - 原像計算困難性, 衝突困難性を満たす

研究の背景

ブロックチェーンとは



- ビットコインにおける送金のイメージ:
  - 手持ちのお札に相手のBitcoinアドレスを書いて, 送金トランザクションを作成
  - そのトランザクションに自分の秘密鍵でデジタル署名をして, トランザクションをビットコインネットワークに流す感じ
- **ブロックチェーン: 時系列ハッシュチェーン**
  - いくつかのトランザクション(送金履歴)をひとまとめにしてブロックを作る
  - どこかのブロックを改ざんすると, 次のブロックのヘッダに含まれるハッシュ値が変わるので改ざん検知可能

研究の背景

ブロックチェーンとは

- **コンセンサスアルゴリズム**: Proof of Work
- **マイニング**: ブロックヘッダの一領域(nonce)に適当な値を入れて, ブロックのハッシュ値の先頭n桁を0にしようゲーム
  - 見つかる確率は$\frac{1}{2^n}$なので, nが大きいと大変困難→時間がかかる
- 手前のブロックを改ざんしようと思ったら, 大変な計算量を投入しないといけない→改ざんが現実的に困難

研究の背景

ブロックチェーンとは

- **スマートコントラクト**: ブロックチェーン上にプログラムコード・Stateも載せる
  - ブロックチェーンを, コンピュータのメモリとみなすイメージ
  - 状態遷移をトランザクションで引き起こす
- DApps(スマートコントラクトを用いたアプリ)が流行っている(?)
  - NFT, DeFiなどもスマートコントラクトで実現されている

研究の背景

ブロックチェーンが実現したもの

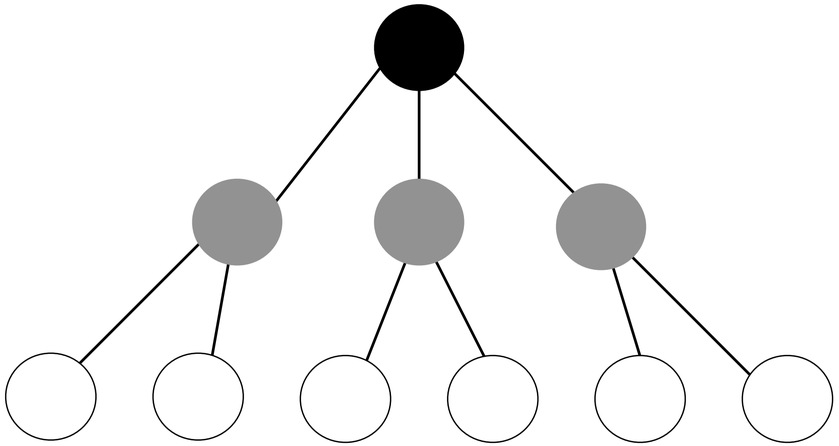
- 電子通貨の二重使用問題の解決
- 共有台帳への分散合意
- デジタル署名による送金
- 分散P2Pネットワークシステム
- **信頼できる第三者が不要なトラストの実現**

研究の背景

信頼できる第三者が不要なトラストの実現

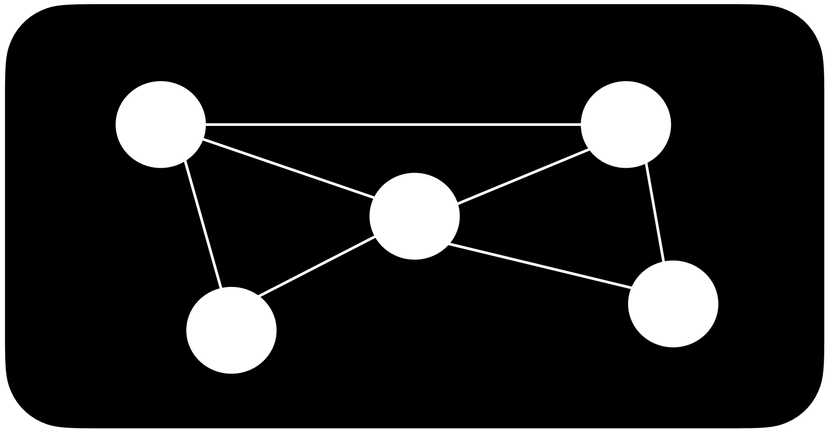
- 互いのどのノードも信頼し合っていない状況でもシステムが動く仕組みを構築
  → システム全体に対するトラスト(共同幻想)が発生し, 仮想通貨に価値が付く

階層型構造のトラスト



SSL/TLSのトラストチェーンはこういう感じ

トラストレスなトラスト (パブリックチェーン)



個々の主体はトラストされていないが, ネットワーク全体はトラストされている

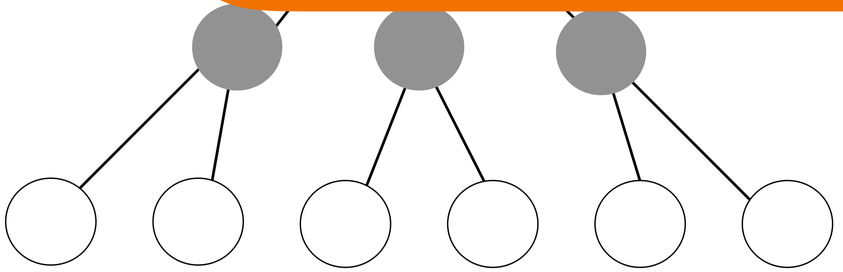
信頼度合い 高 → 低

研究の背景

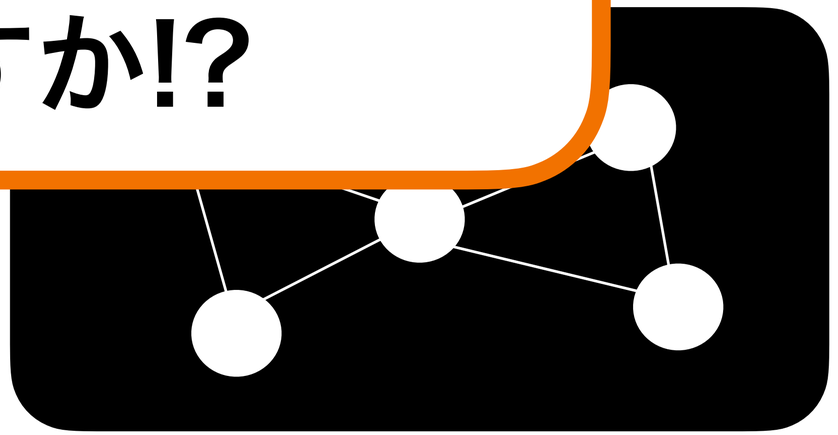
信頼できる第三者が不要なトラストの実現

- 互いのどのノードも信頼し合っていない状況でもシステムが動く仕組みを構築
  → システム[illegible]に価値が付く

本当に誰も信用しなくていいシステムですか!?



SSL/TLSのトラストチェーンはこういう感じ



ブロックチェーン)

個々の主体はトラストされていないが, ネットワーク全体はトラストされている

信頼度合い 高 → 低

研究の背景

ガバナンス問題

- **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)

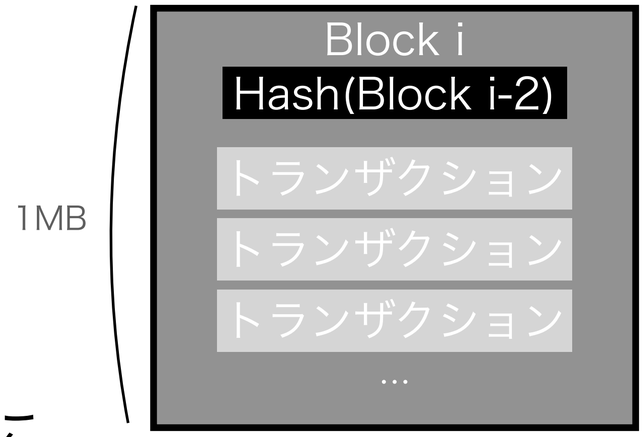
研究の目的と方針

- 現状のガバナンスの問題点を, 事例調査から洗い出す
- 問題点を解決できるようなガバナンス方式を考える (今後)

ケース1: Bitcoin ブロックサイズ論争

ブロックサイズとは

- Bitcoinの**ブロックサイズ**: 1MB
  - 少ししかトランザクションを詰め込めない
  - **スケーラビリティ問題**: ブロック生成時間が約10分になるようnonceのdifficultyが調整されるので, 1時間に6MB分のトランザクションしか捌けない
- ブロックサイズを8MBに拡大させる提案が持ち込まれた



ケース1: Bitcoin ブロックサイズ論争

ブロックサイズ論争の概要

- コミュニティ内で大きな論争になった
  - 賛成派
    - スケーラビリティが向上する
  - 反対派
    - ブロックサイズが大きくなると全体の容量が増えるので, 個人のコンピュータではノード運営が難しくなり, 中央集権的な方向に向かってしまう
- 一部のコア開発者が, 大きなサイズのブロックを受け入れるBitcoin XTを実装し運用
  - XT支持者に対する様々な攻撃等が行われた
  - XTは普及に失敗し, XT開発者は開発の継続をやめた

ケース1: Bitcoin ブロックサイズ論争

明らかになったビットコインガバナンスの問題

- **Governance of the blockchain**の問題が明るみになった
  (Governance by the blockchainとは別)
  - 洗練されていない, 暗黙のガバナンスシステム
  - **少数のコア開発者たちが実装やプロトコルを握り, ノード運営者がそれを採用する権限を持っている** (テクノクラートによるガバナンス)
    - 当然, 新しいコードの提案は誰でもできるが, それが採用されるかどうかはコア開発者次第

ケース2: The DAO事件

概要

- The DAO事件
  - Ethereum上のスマートコントラクトにバグがあり, 約360万ETHが盗まれた
  - Ethereumのコアメンバーは, 盗まれたトランザクションをなかったことにする**ハードフォーク**を提案
    - 多くのノードが受け入れ, なかったことになった
    - 一部のノード運営者は反発し, Ethereum Classicという別チェーンになった

ケース2: The DAO事件

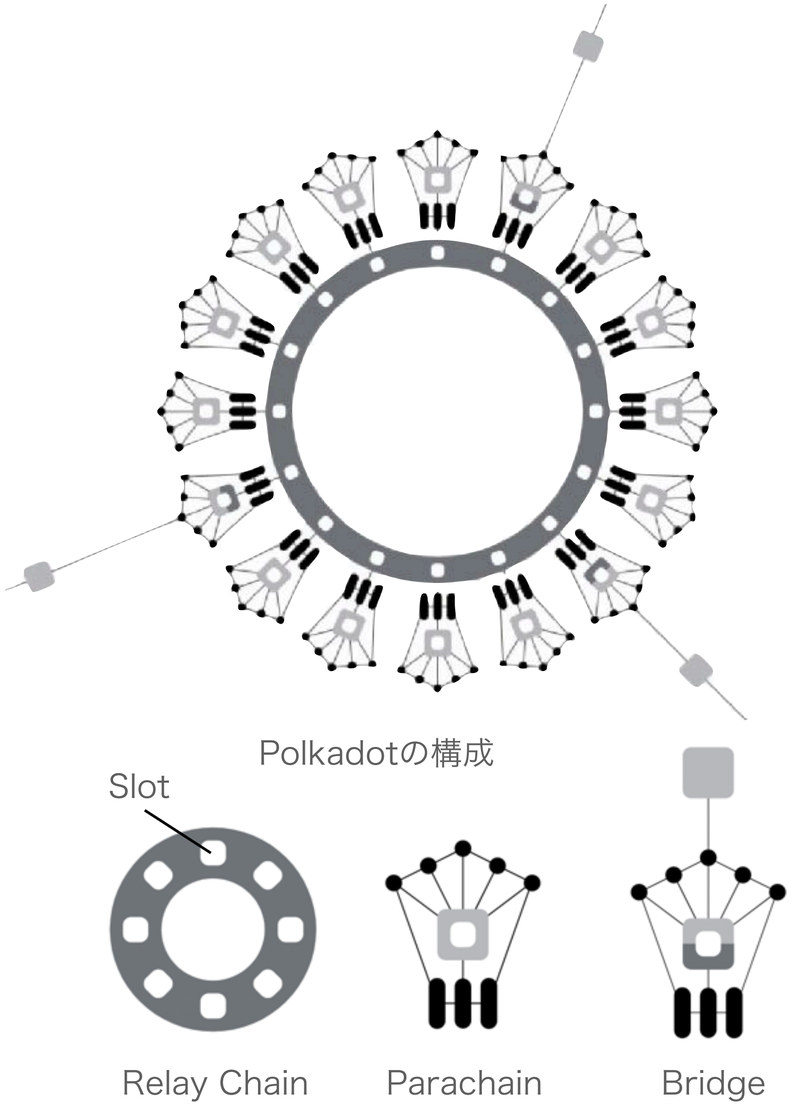
問題

- **コア開発者とノード運営者が大きな力を持ち, 過去の取引をなかったことにしてしまえることが証明されてしまった**
- Ethereum Classicと新Ethereumの間でハードフォークが起こった
  - トークンが2倍!?
  - 議論になるたびに毎回ハードフォークなどをしていたら, どんどんチェーンが枝分かれしていってしまう

ケース3: 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



ケース3: Polkadot

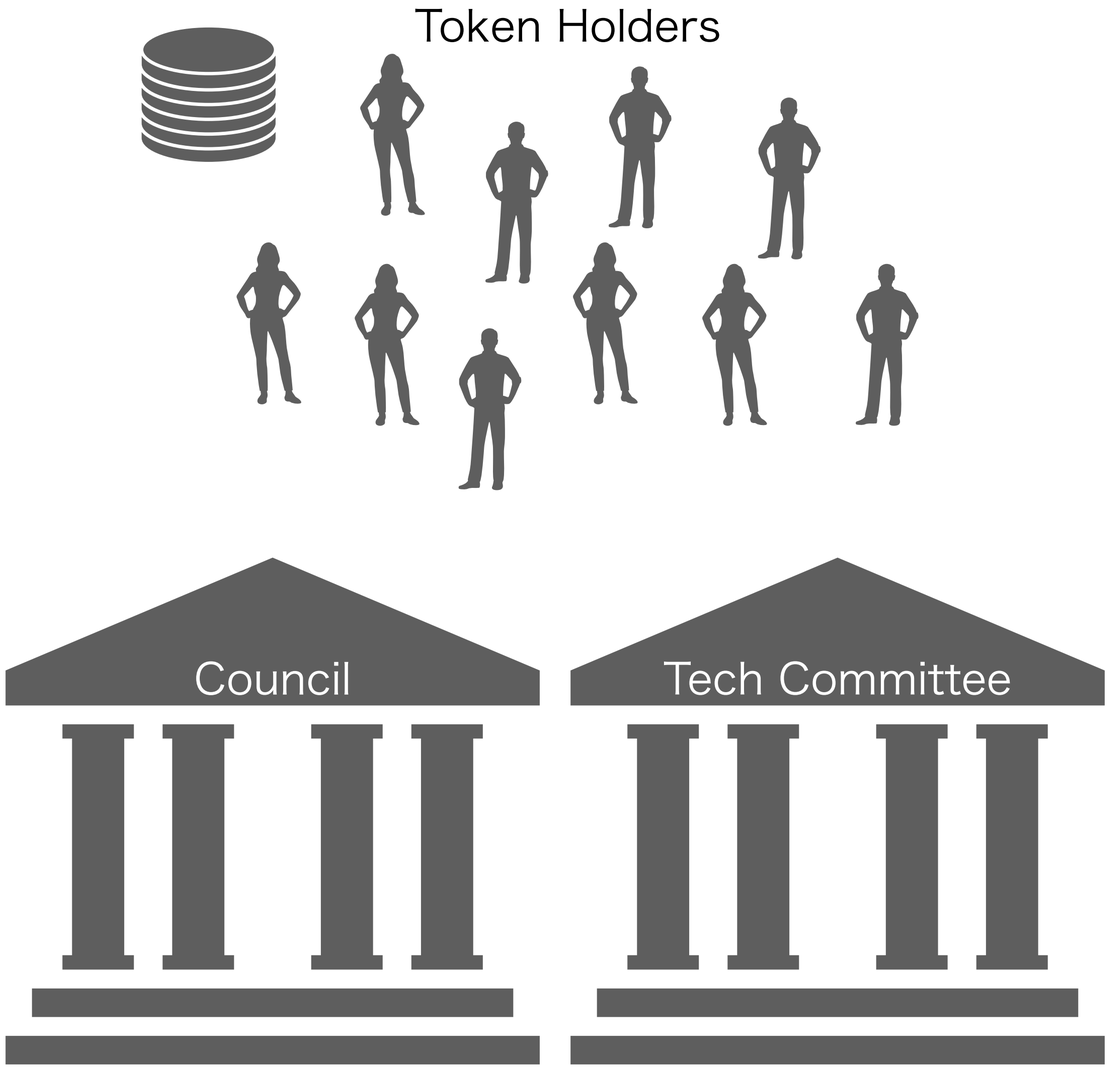
フォークレスアップグレード

- 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**

ケース3: 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

ケース3: Polkadot

提案の発議

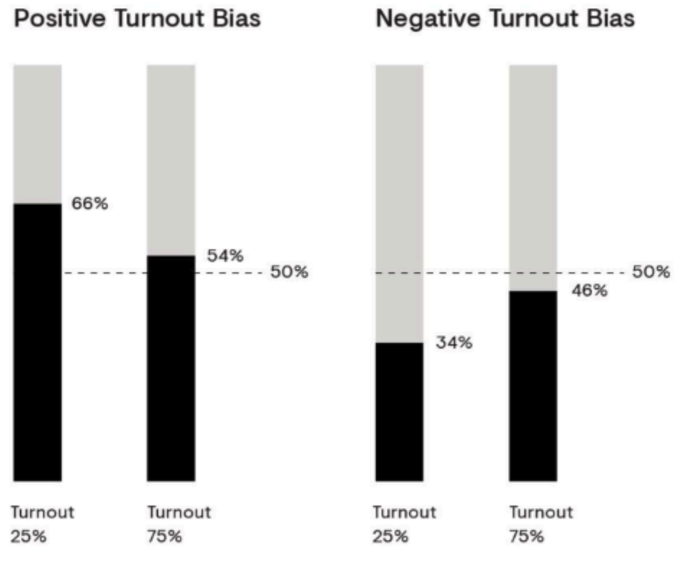
- 提案の種類
  - **Public referenda**
    - 一定の期間トークンを預けることで投票の提案ができる
    - 同額のトークンを預けることで賛成できる
    - 最も賛成を得た提案が, 次の投票プロセスに回される
  - **Council referenda**
    - Council発の議案は即次の投票プロセスに回される

ケース3: 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



ケース3: 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**

今回分かった問題点

- 暗黙的なガバナンス構造は混乱を招き, テクノクラート優位な政治を生み出す
- ガバナンス構造を有しているチェーンはあるが, 投票にトークンを使っているものが多く, お金持ち優位な政治になってしまう

今後の予定

- 現状だとケースを調べただけになっているので, 何らかのフレームワークを用いて現状のガバナンスの問題点をもう少し洗い出していきたい
  - どうすれば?
- 投票によらない適切なガバナンス形式を模索していきたい
  - どうすれば?

参考文献

- Carter, N. (2018, June). An overview of governance in blockchains. Presentation at Zcon0 2018, Montreal, Canada.
- Pelt, Rowan van, et al. "Defining blockchain governance: A framework for analysis and comparison." Information Systems Management 38.1 (2021): 21-41.
- De Filippi, P., & Loveluck, B. (2016). The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet policy review, 5(4). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691
- ZDNet Japan.「The DAO」ハッキング事件、ブロックチェーンの“巻き戻し”対応に賛否両論 https://japan.zdnet.com/article/35085933/
- Polkadot Wiki: https://wiki.polkadot.network/
- Polkadot Whitepaper: https://polkadot.network/PolkaDotPaper.pdf
- How Nominated Proof-of-Stake will work in Polkadot, Alfonso Cevallos, Web3 Foundation: https://medium.com/web3foundation/how-nominated-proof-of-stake-will-work-in-polkadot-377d70c6bd43