

PoS型ブロックチェーンにおける公平分配によるステーク分散の設計と評価

先進ネットワーク研究室
屋敷圭太

ブロックチェーン

■ ブロックチェーン

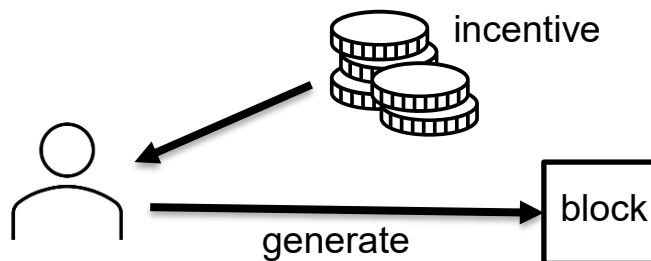
- 複数のコンピュータ間の台帳上で共有して管理
- 取引の改ざんが困難

■ コンセンサスアルゴリズム

- ブロックチェーン内のノード間で合意を形成するためのルール
- Proof of work
 - 計算能力を競う競争型合意
 - ex. Bitcoin
- Proof of stake
 - 保有資産を基盤とした選出型合意
 - ex. Ethereum

PoS: インセンティブメカニズム

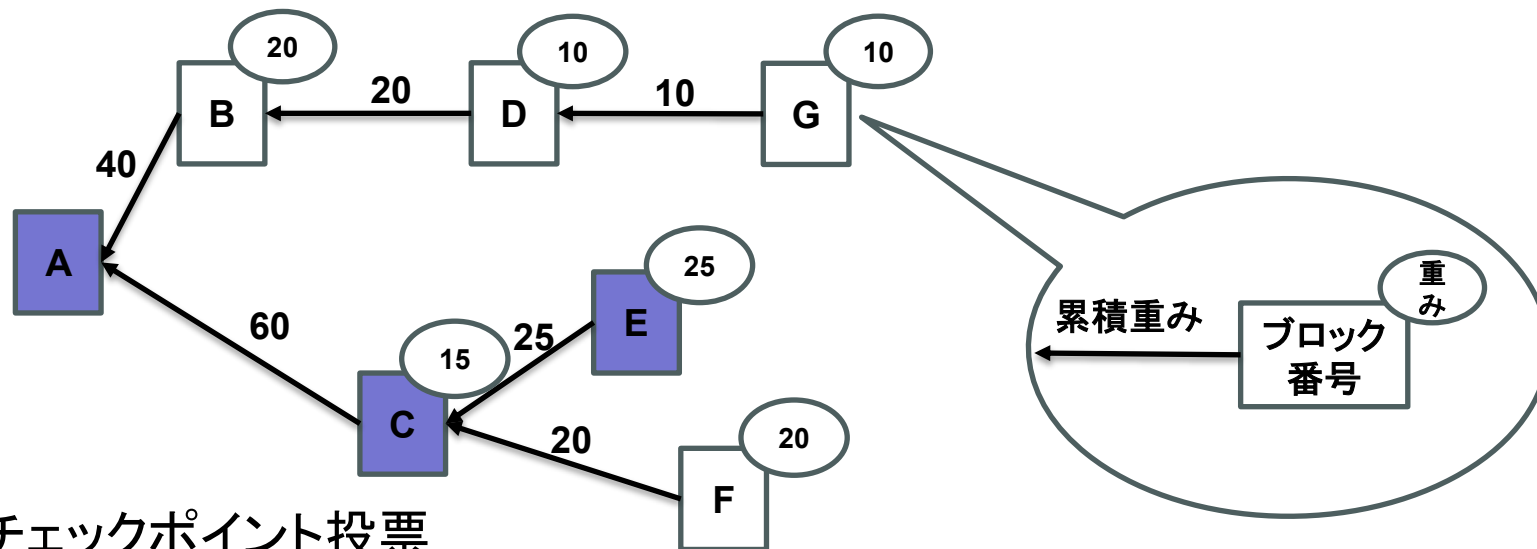
- バリデータ(ノード)はブロックを生成することでインセンティブ獲得



- ステーク(保有資産)量の多いバリデータ
 - ステーク量に応じてブロック生成に伴うインセンティブが増加
 - ブロック生成に指名される確率増加
- 従来インセンティブ式: $I_i = S_i$
 - I : インセンティブ
 - s : ステーク
 - i : バリデータ
- ブロックチェーンネットワーク内でステーク量の偏りが発生

ステーク量の大小に伴う支配力の差異

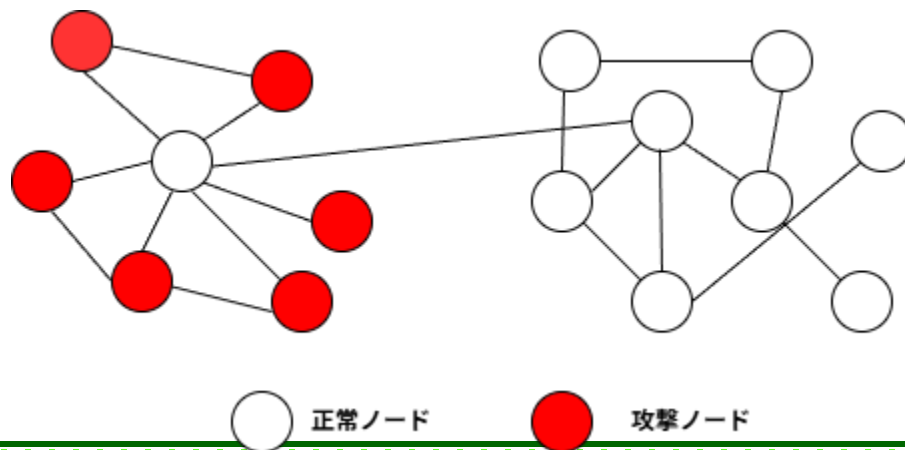
- ステーク量でブロック生成バリデータの選出確率が変化
- チェーンの枝分かれ(フォーク)が発生した時累積重みに基づいて正当なチェーンを決定
 - ステーク量に基づいて投票の重みが決定



- チェックポイント投票
 - 正当なチェーン決定後, 全体のステーク量2/3以上の投票で最終チェーンを決定
 - ステーク量の多いバリデータは投票の影響力大

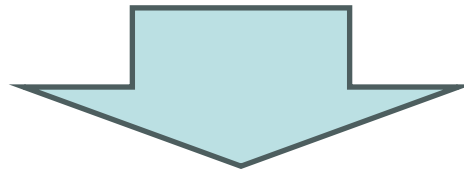
Sybil攻撃

- 単一の攻撃者が複数の偽ノードを生成
 - 複数の新規バリデータをネットワークに投入
 - バリデータを用いてブロック生成, ブロック投票で不正に操作
- 分散化に伴う課題
 - ネットワーク内のステークが分散
 - sybil攻撃に脆弱
 - 新規に参加する攻撃者がsybil攻撃に必要なステークを得やすくなる



研究目的

- ネットワークの中央集権化
 - 特定のバリデータにステークが集中



- ステーク分散を目的としたインセンティブ手法
 - ステークの中央集権化解消によるsybil攻撃耐性弱
- Sybil攻撃バリデータ検知手法の提案

インセンティブ式

■
$$Incentive = \frac{validator_stake^\alpha}{\sqrt{All_validator_stake}} * C$$

■
$$\alpha = \frac{1}{1 + \beta * \frac{validator_stake}{All_validator_stake}}$$

■ $validator_stake$: バリデータの保有するステーク量

■ $All_validator_stake$: ネットワーク全体のバリデータのステーク量

■ C : ブロック生成報酬の基準額

■ β : 調整変数

■ 各バリデータのステーク量を α で調整

■ ステーク量の多いバリデータのインセンティブ量を緩和

■ 新規参入者のインセンティブ量増加

クラスタリングを用いた攻撃者検知

- 以下の特徴量を用いてユーザをクラスタリング
 - 特徴量の定義
 - フォーク発生時のブロック投票における投票の偏り度
 - 過去のブロック生成数
- 攻撃者検知ロジック
 - 正常バリデータ
 - ブロック生成者のステーク量, 過去のブロック生成履歴に基づいて投票先を選択
 - 攻撃者
 - 自身が生成したブロックに投票
 - 複数の偽バリデータを用いて投票

評価条件

- 計算機シミュレーションにより評価
 - ブロック生成数: 3200ブロック
 - バリデータ数: 128
- 新規バリデータステーク量
 - 従来手法, 関連研究(LSW)と比較
→インセンティブ式: $I_i = \log s_i$
- 攻撃者検知率
 - 攻撃者割合: 全バリデータの10%
 - 新規参入者割合別に評価
 - シナリオA: 17%, シナリオB: 41%, シナリオC: 69%

評価: ステーク量・検知率

■ ステーク量

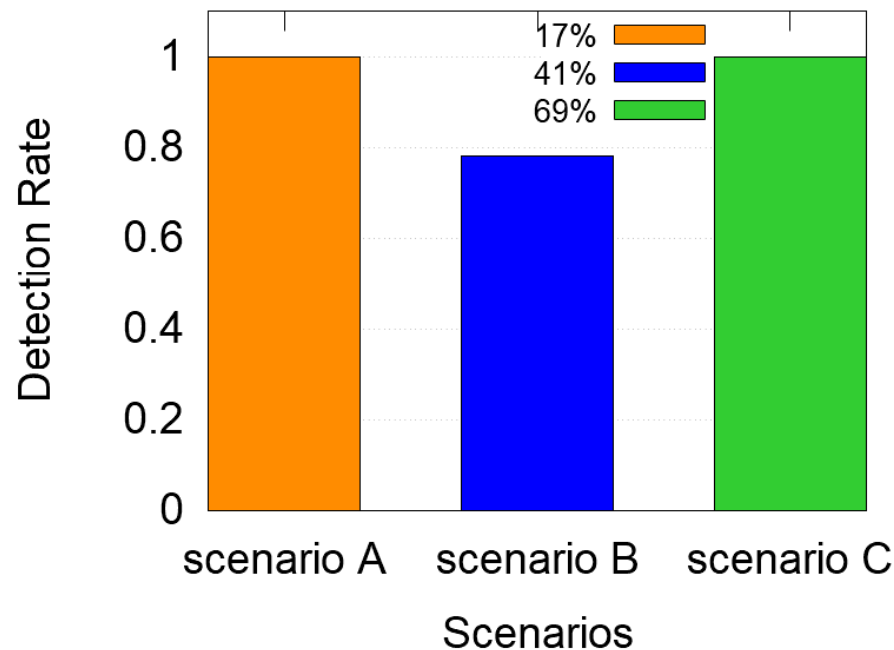
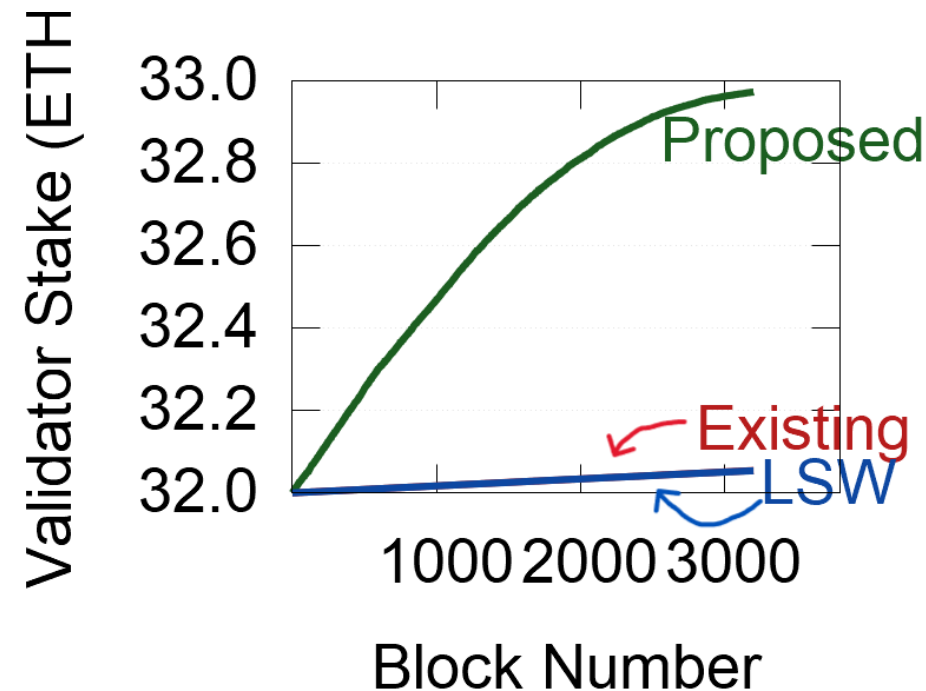
- 提案手法のステーク量が最も増加

- Existing < LSW < Proposed

■ 攻撃者検知

- シナリオBの検知率78%

- ブロック生成率の低い新規バリデータと攻撃者の投票行動が類似→誤検知発生



まとめ

- ネットワークの中央集権化を解消するインセンティブ式, sybil 攻撃検知手法
- 今後の予定
 - Sybil攻撃時の獲得報酬を各手法で比較・評価