Analysis of Eclipse-Attack Vulnerability on Single Global Ledger Cryptocurrencies

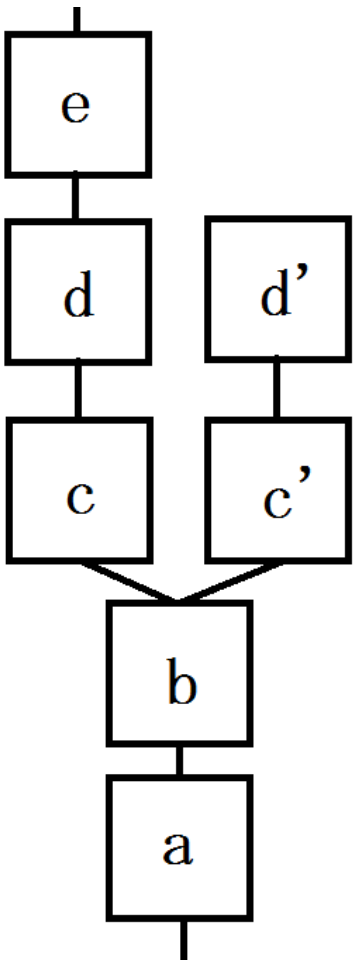
単一グローバル台帳暗号通貨のエクリプス攻撃脆弱性分析

政策・メディア研究科
修士2年　澁田　拓也

はじめに

- Bitcoin等の単一グローバル台帳暗号通貨が下位のネットワークにエクリプス攻撃に対する脆弱性を抱えている可能性
- Bitcoinに対するエクリプス攻撃のシミュレータを作成
- シミュレーションの結果を検証し、単一グローバル台帳暗号通貨のエクリプス攻撃に対する脆弱性の度合いを提示

Blockchain fork



- 単一グローバル台帳暗号通貨では、短期的に別の内容の複数のBlockが同時にネットワークに伝搬する事があり、その現象はBlockchain Forkと呼称されている
- Blockchain Forkの発生は、Bitcoinネットワーク全体での分散合意形成の短期的失敗を示している
- Blockchain Fork発生後、同順位のブロック群の後に新たにブロックが採掘された方を認知したノードは採用する

Bitcoinに関する認識の誤り

- 現状のBitcoin実装ではDNSに問い合わせしない
- getaddrとaddrメッセージは、隣接ノードリストでは無く、存在を知っているノードの一覧の送受信を行う
- addrメッセージの内容は一律では無く、無作為に抽出される
- 当該既知ノードリストの管理には複雑な機構が用いられている

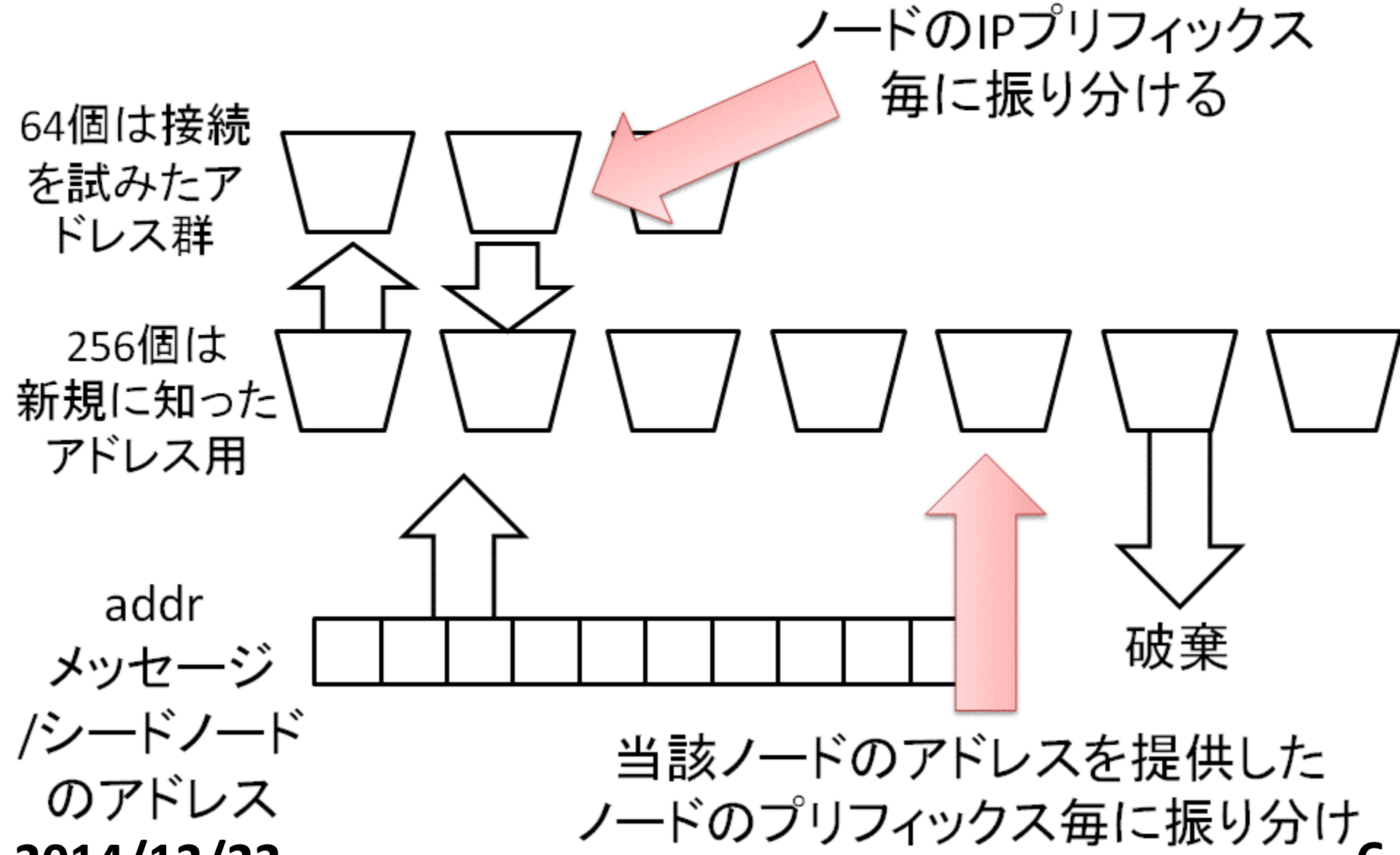
Bitcoinの既知ノードリスト管理機構

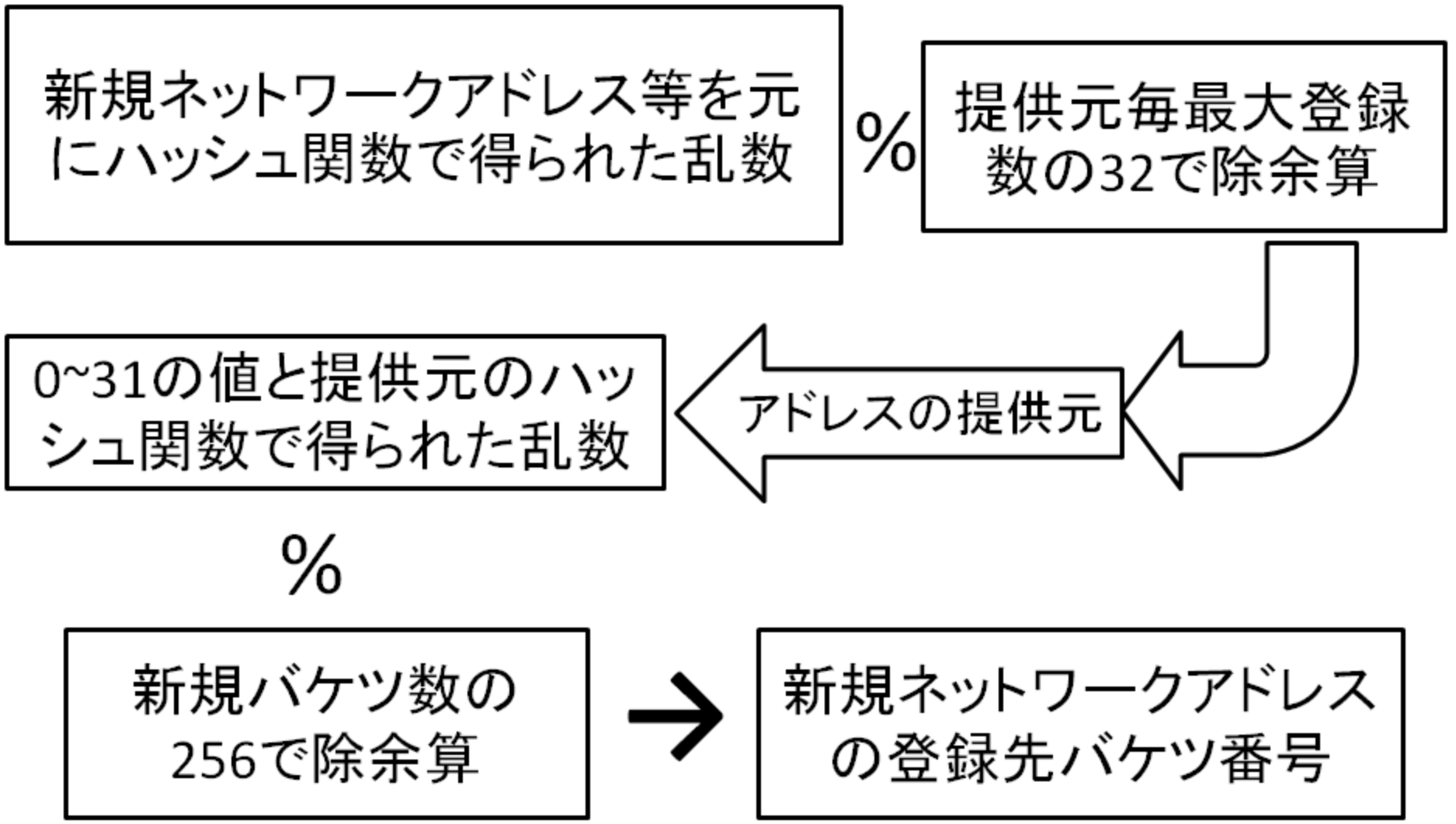
- 限られた数のネットワークアドレスのみの保有を行う事で公式クライアント実装の 起動の遅延を防ぐ

結託攻撃を防ぐため:

- 攻撃者が同一ネットワークセグメントに存在する悪しきノードのネットワークアド レスでネットワークアドレスのデータベースを汚染する事が出来無い事
- 攻撃者が幾重もの addr メッセージを用いて善良なノードのネットワークアドレス データベースを汚染しようとしても、限られた範疇の影響しか受けないこと

Bitcoinにおける既知ノードリスト




新規ネットワークアドレス等を元にハッシュ関数で得られた乱数
%
提供元毎最大登録数の32で除余算
0~31の値と提供元のハッシュ関数で得られた乱数
アドレスの提供元
%
新規バケツ数の256で除余算
新規ネットワークアドレスの登録先バケツ番号

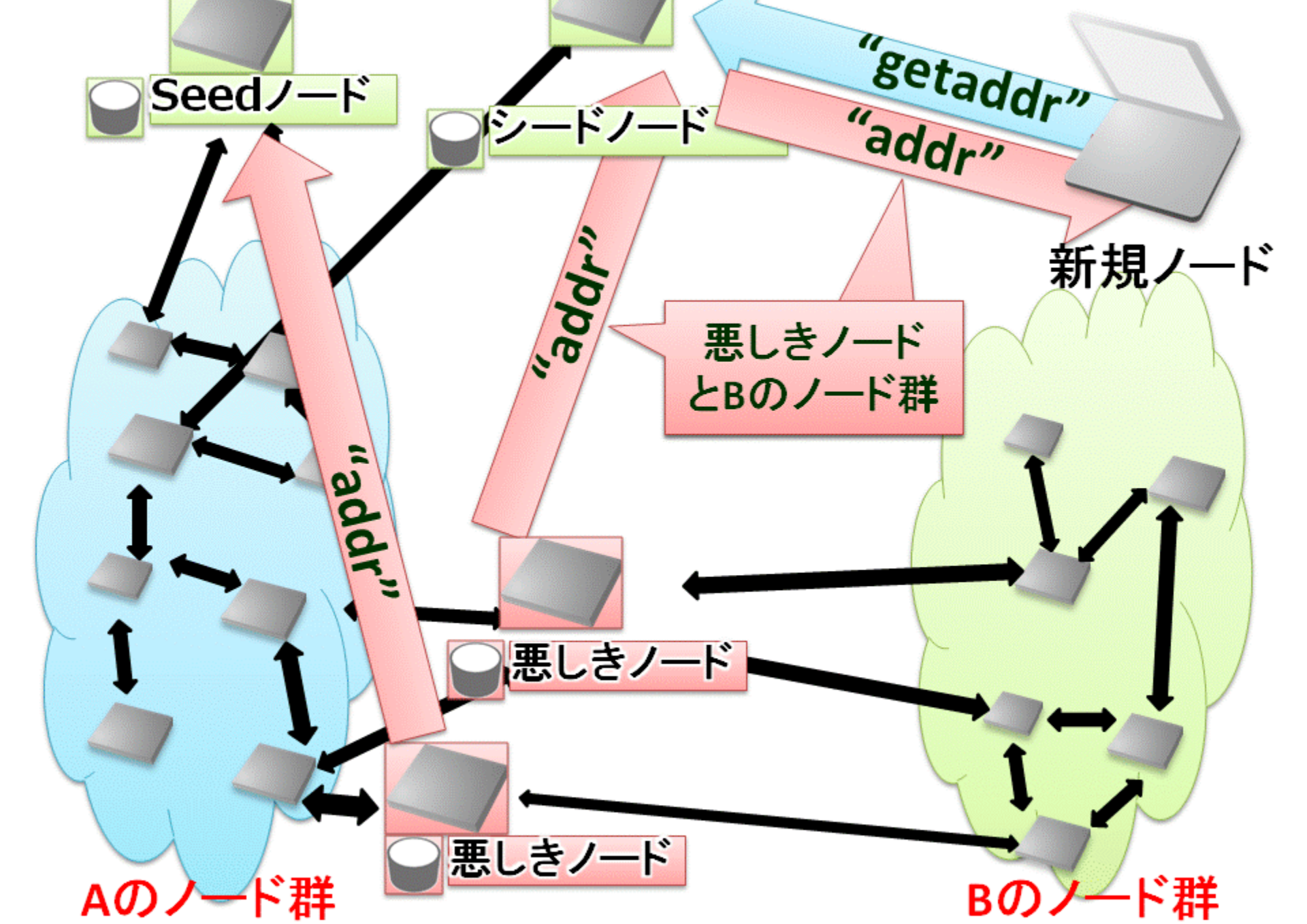
エクリプス攻撃のシナリオ

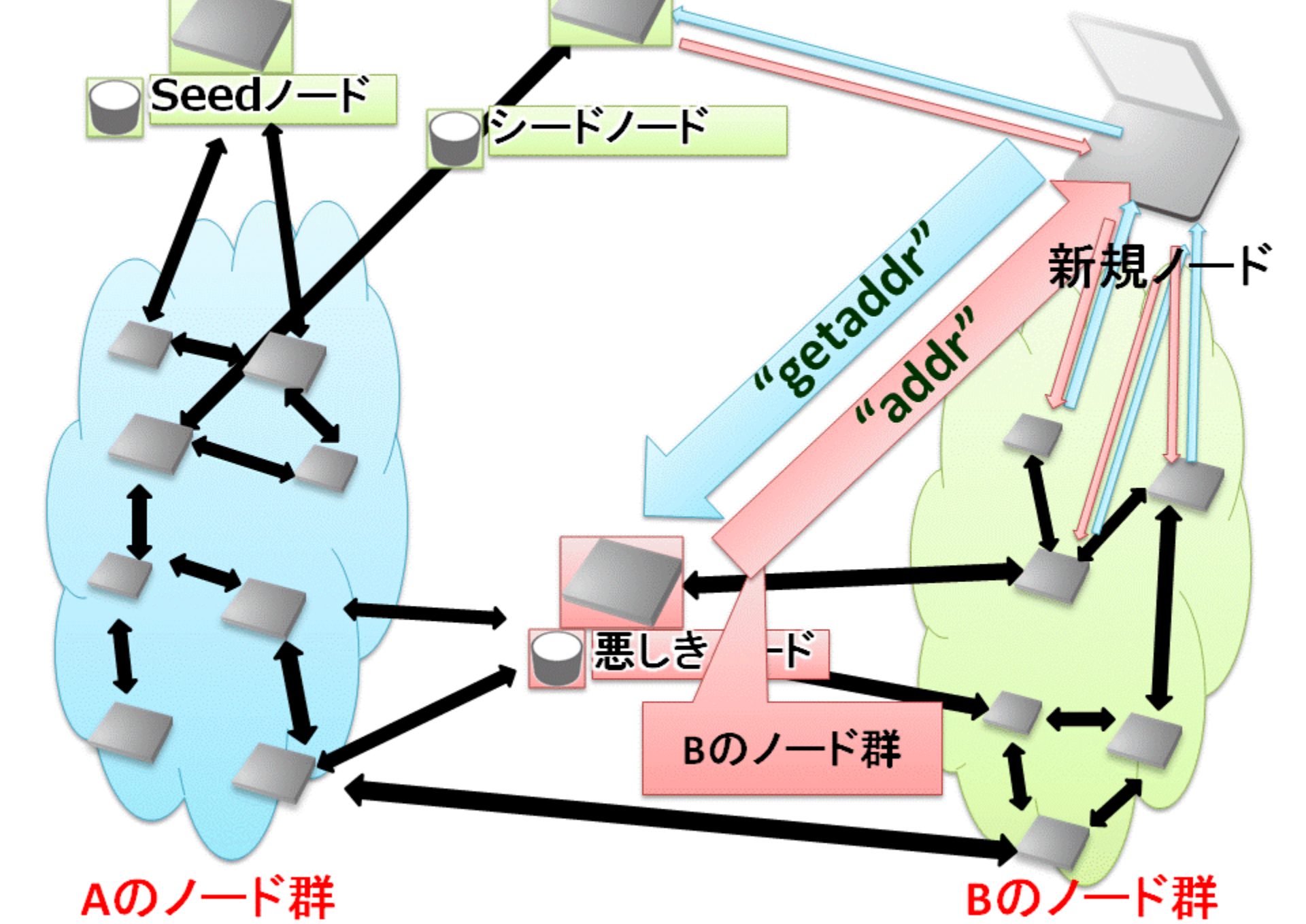
攻撃の目的はBitcoinの貨幣としての可用性と信頼を貶める事

もしくは

Bitcoinネットワークの分断、そしてそれに基づく次ブロック採掘における自計算力の相対的増加

- 一般ノードとして攻撃ノードをネットワークに接続して攻撃


Seedノード
シードノード
“getaddr”
“addr”
新規ノード
“addr”
“addr”
悪しきノード
とBのノード群
悪しきノード
悪しきノード
Aのノード群
Bのノード群


Seedノード
シードノード
新規ノード
“getaddr”
“addr”
悪しき
Bのノード群
Aのノード群
Bのノード群

考察で作る予定のグラフ

中のデータは現状嘘です

シミュレータのパラメータ

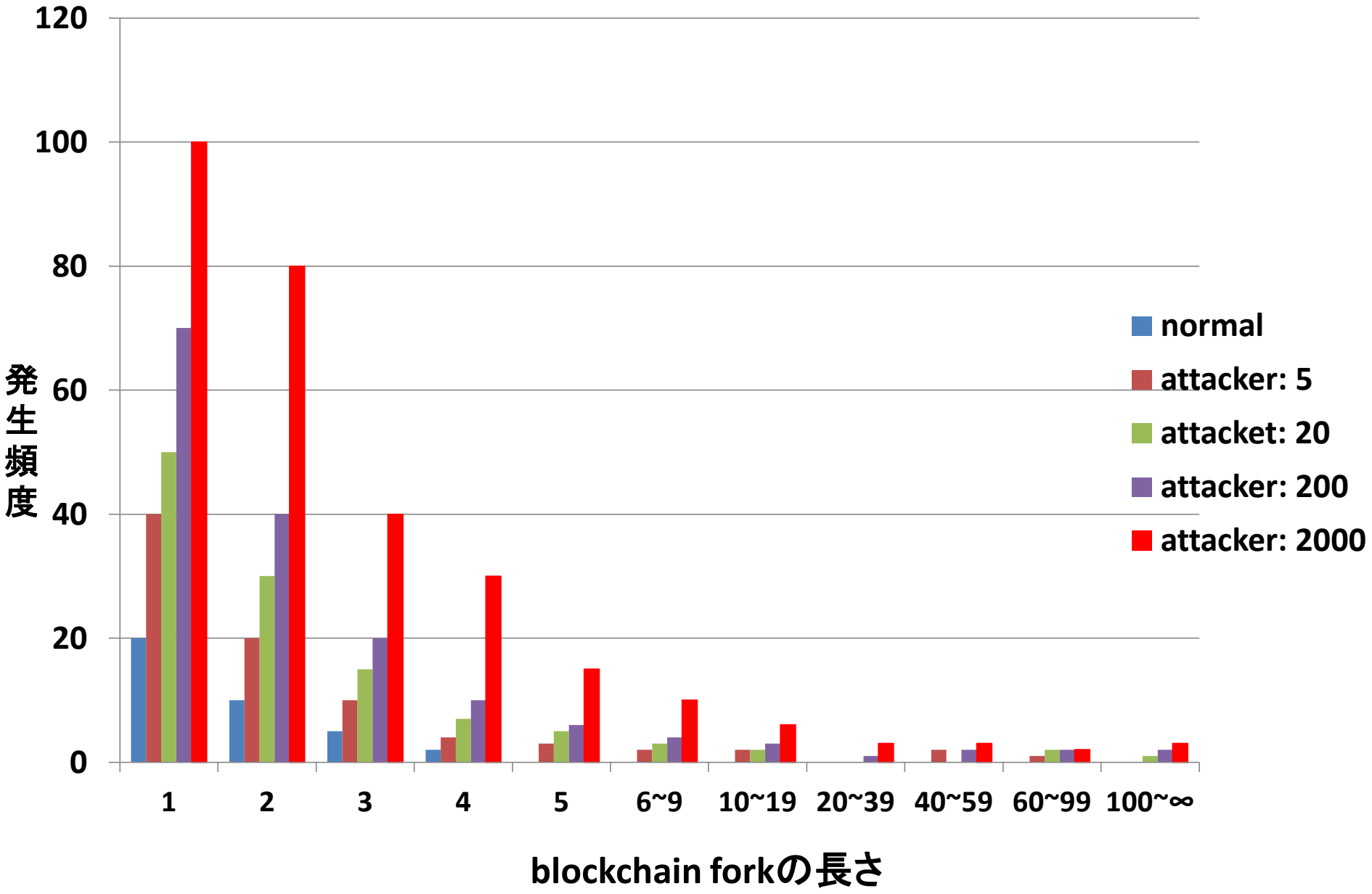
- シミュレートする時間
- 全ノード数
- シードノードの数
- 一般ノードのTTL
- シードノードのTTL
- 攻撃者ノードの数
- 攻撃者が一般ノードを割り振るグループA-Bのノード数の比率

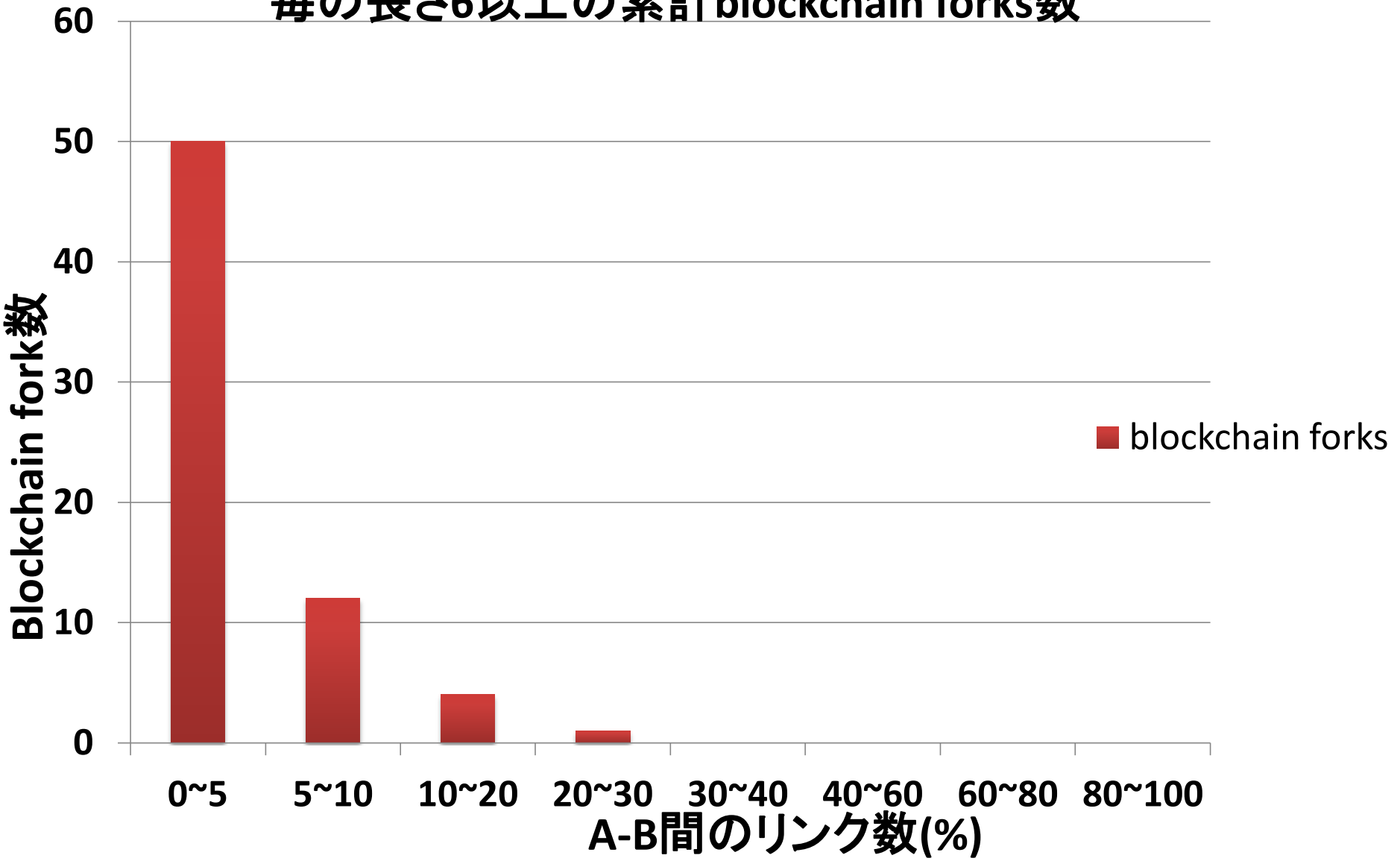
Blockchain ForkとBitcoin

- 現状実際のBitcoinネットワークで、バグ以外が原因の最長のblockchain forkは長さが4
- 取引で得られた貨幣の利用は慣習上6ブロック分の長さ経過後
- 新規ブロック採掘報酬で得られる貨幣が利用できる迄の期間は規則上100ブロック分経過後

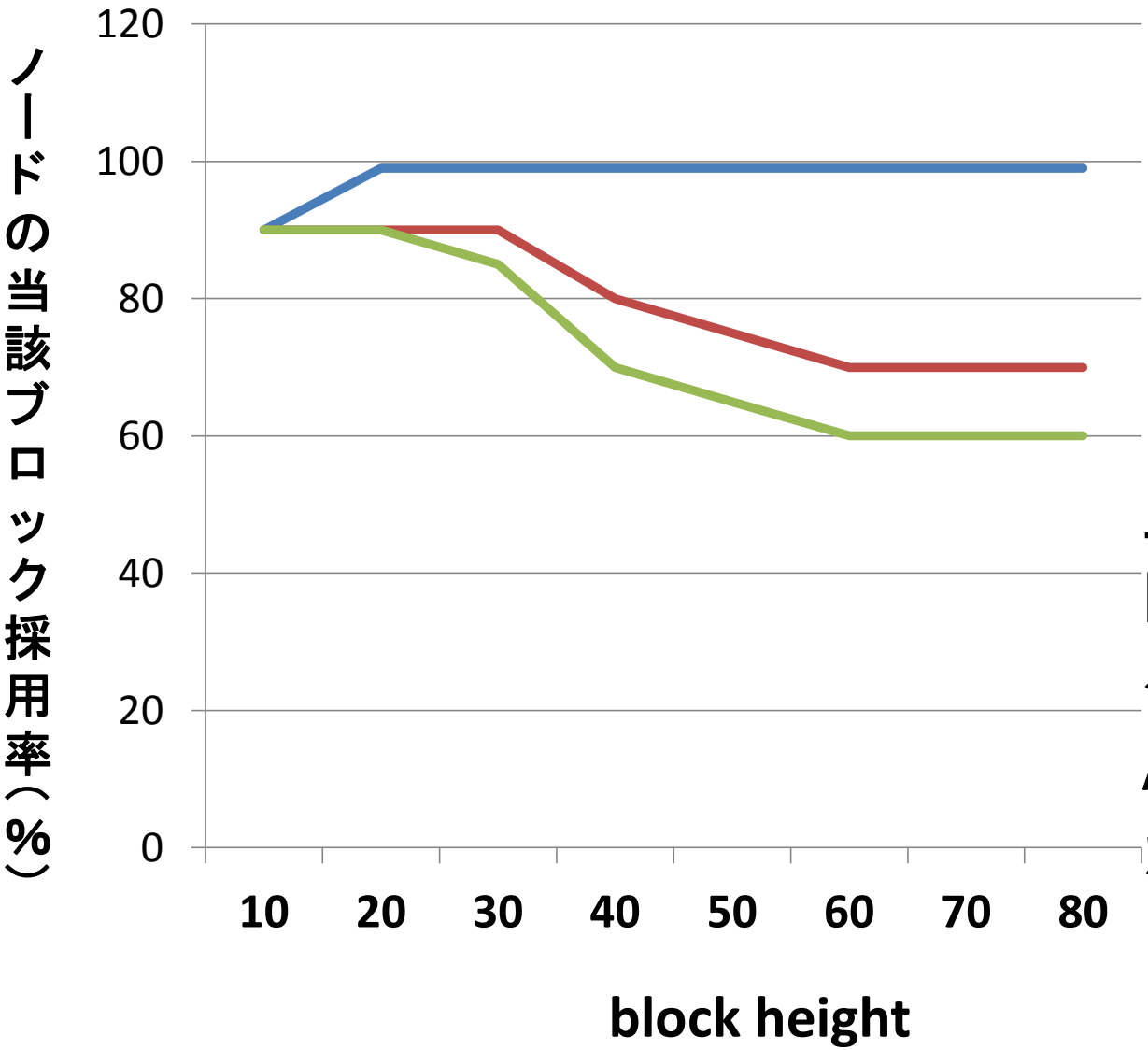
- 6ブロック以上のblockchain forkが頻出すれば利用者に混乱が発生する
- Blockchain Forkが100ブロック継続すればエクリプス攻撃によりBitcoinの貨幣及び決済システムとして可用性と信頼を貶められた事となり

Blockchain fork長さごと発生頻度



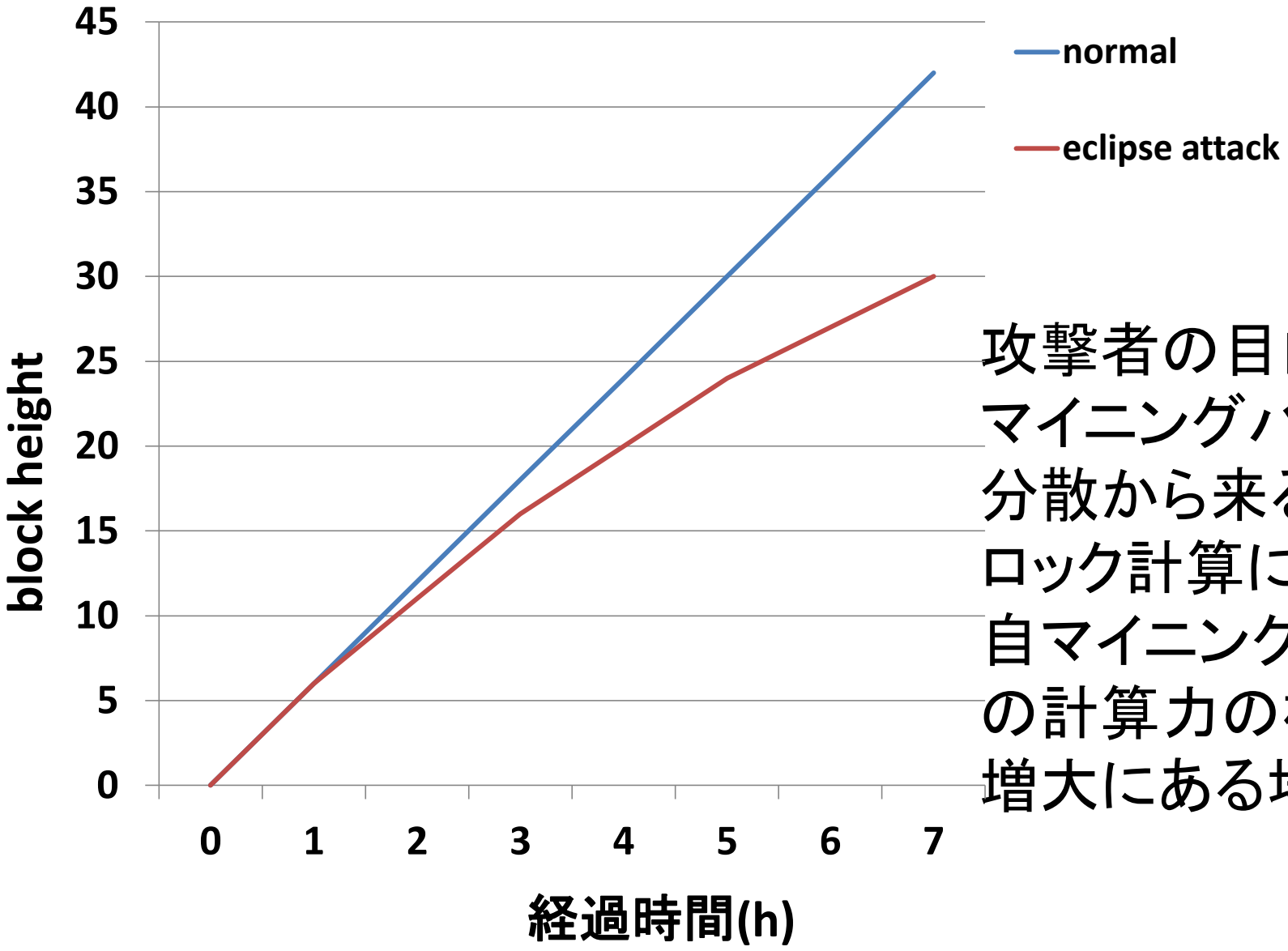

全体のリンク数に対するA-B間のリンク数の割合
毎の長さ6以上の累計blockchain forks数
60
50
40
30
20
10
0
Blockchain fork数
blockchain forks
0~5
5~10
10~20
20~30
30~40
40~60
60~80
80~100
A-B間のリンク数(%)

block毎の採用ノードの割合

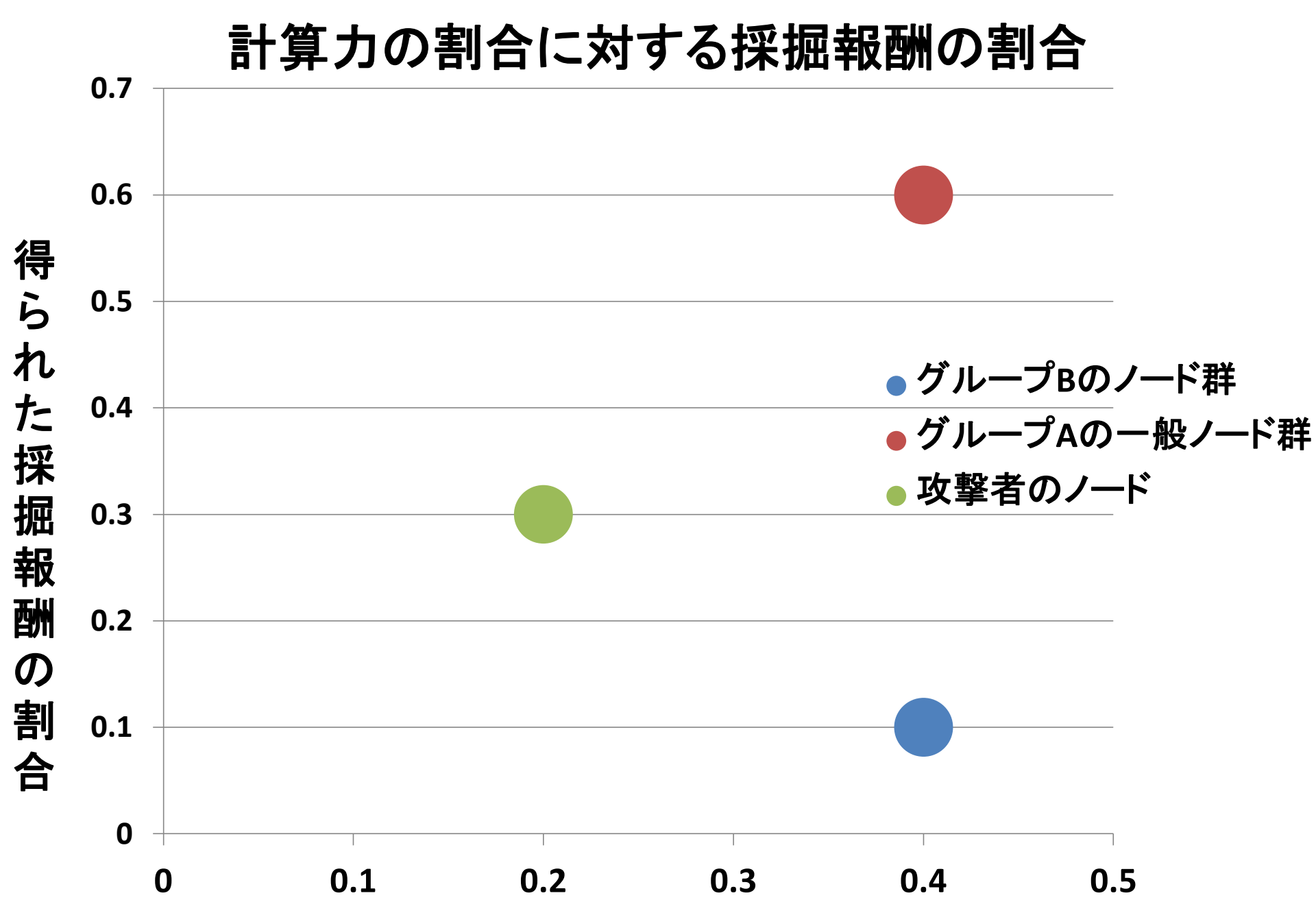


エクリプス攻撃成功時、どれだけブロックの伝搬とグループA-Bのノード数の比率が近似しているか

時間経過毎のblock heightの増加



攻撃者の目的が:
マイニングパワーの分散から来る新規ブロック計算に占める自マイニングプールの計算力の相対的増大にある場合


計算力の割合に対する採掘報酬の割合
得られた採掘報酬の割合
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.1
0.2
0.3
0.4
0.5
グループBのノード群
グループAの一般ノード群
攻撃者のノード

当研究の社会的意義

- Blockchainを用いた暗号通貨はBitcoinに限らず、それから派生したaltcoinにも適用されている
- またEthereumなどの通貨システム以外のシステムにて分散合意形成の手法として応用もされている
- それらに関してエクリプス攻撃の可能性が存在し、脅威であるかをシミュレーションにより検証し、提示する事が当研究の目的である

TODO

- 短期的目標
  - メモリ利用の過多が発生するバグの修正
  - 実験
  - 考察
  - 評価

まとめ

目的:

- Bitcoinがエクリプス攻撃に脆弱な可能性がある
- シミュレーションを行い、検証し、結果を提示する

進捗:

- 実装はメモリの利用過多が生じるバグ以外は概ね完了

TODO:

- 実験
- 考察
- 評価