Eclipse Attack on Single Global Ledger Cryptocurrencies

単一グローバル台帳暗号通貨に対するエクリプス攻撃

政策・メディア研究科
修士2年　澁田　拓也

はじめに

- Bitcoin等の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

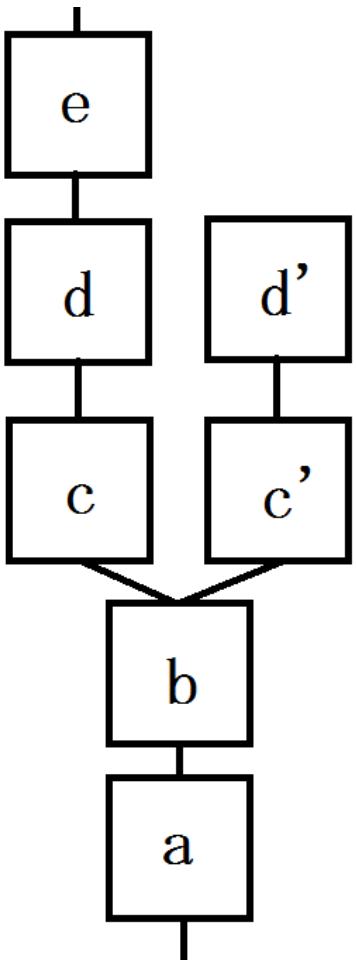
- 先行研究によりエクリプス攻撃への脆弱性が実証されたが、提案している改善策が問題を抱えており、他のエクリプス攻撃手法に対して未だ脆弱である可能性がある

- 双方のエクリプス攻撃に対する長期的な視野に立ったスケーラブルな改善策の考察を行う

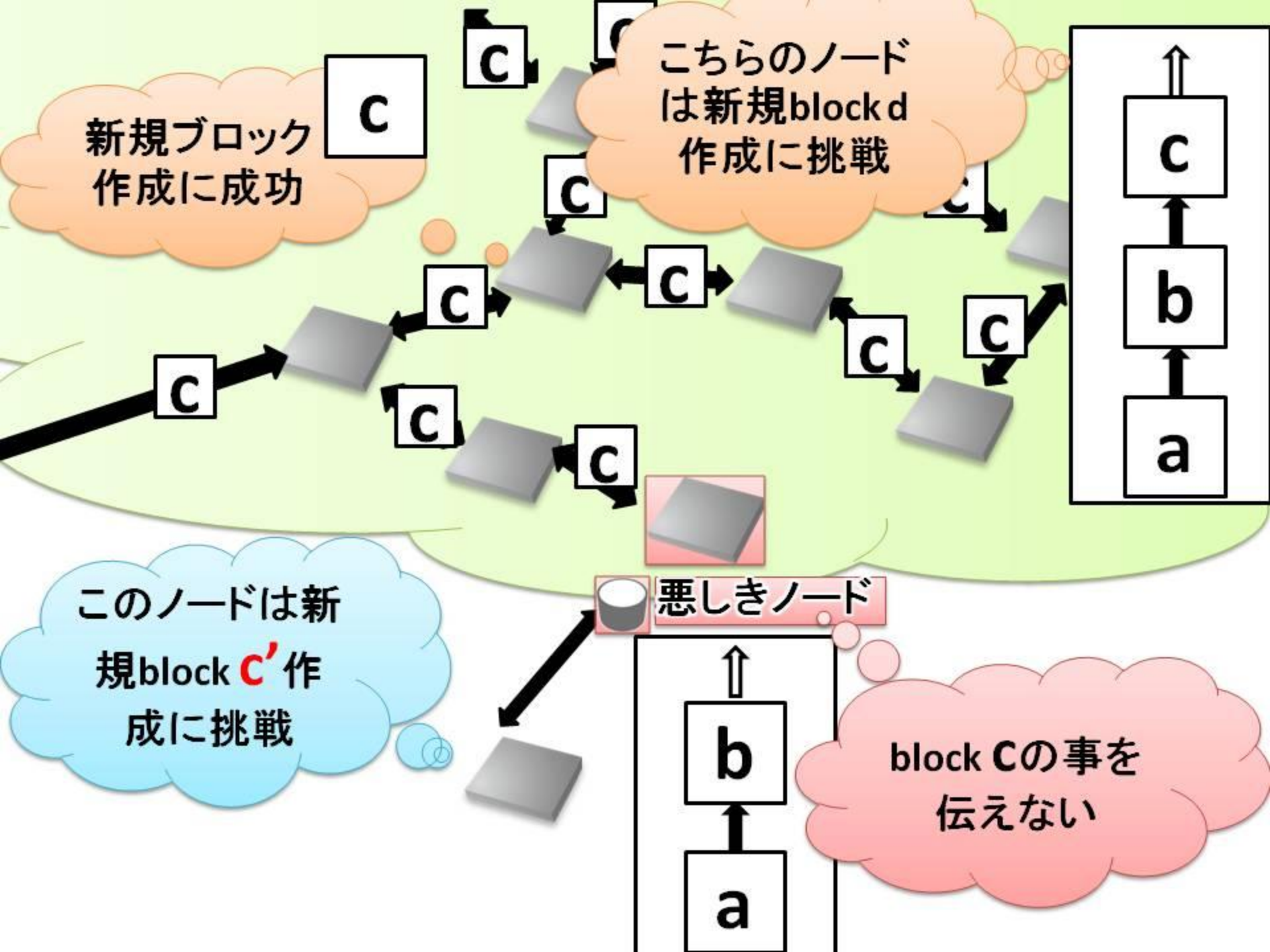
Bitcoin

- 2009年のオープンソースソフトウェアとしての公開以降商取引などが活発化
- Litecoin等の派生通貨を導出
- Blockchain と呼ばれるシステム全体の台帳により取引の記録
- Blockchainはblockとよばれる1単位毎により台帳に追記
- Blockの追記には報酬が伴う:
  - 多くのノードが競争的にblockの作成に参加

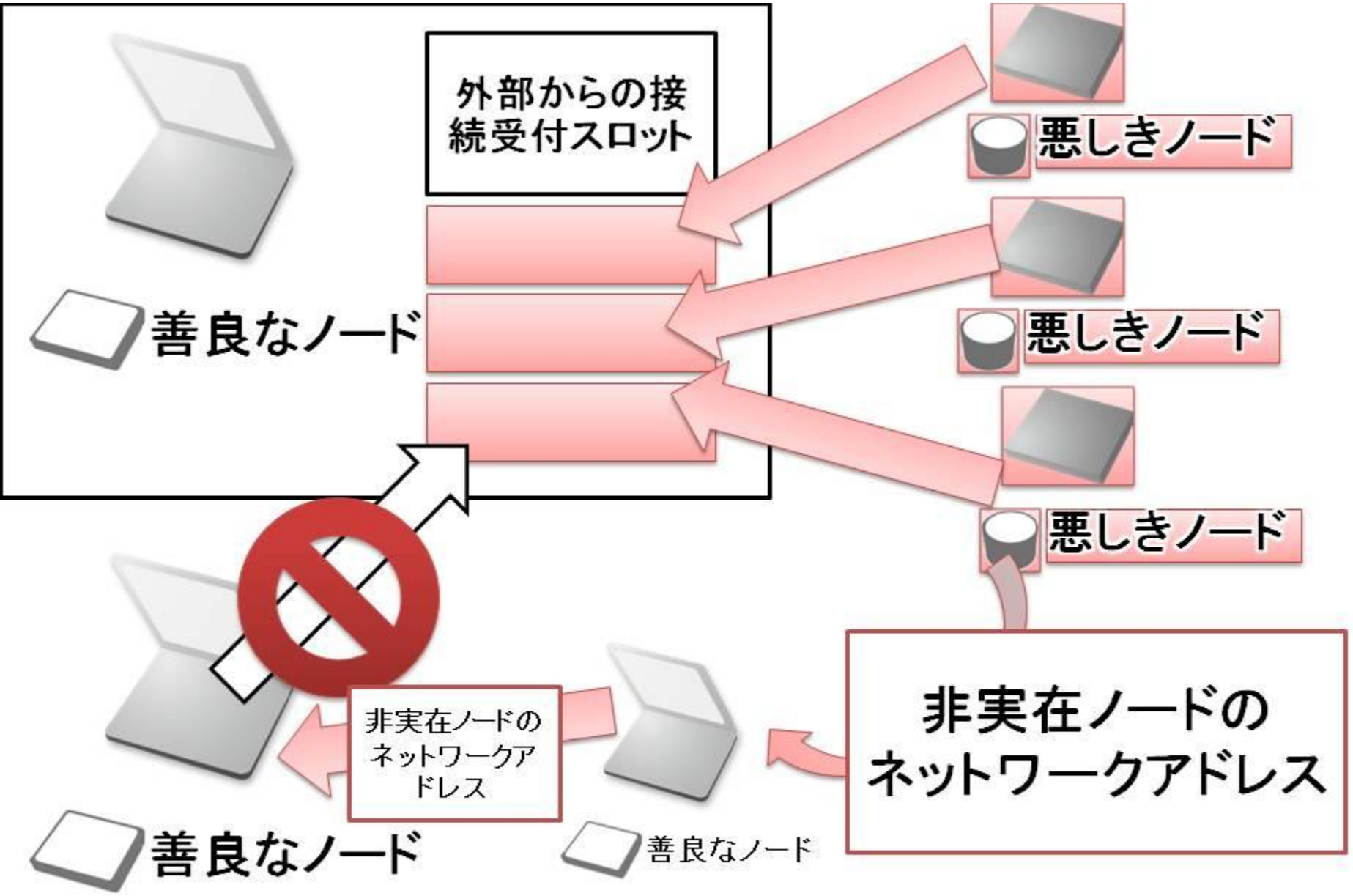
Blockchain fork



- Bitcoin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


新規ブロック
作成に成功
c
こちらのノード
は新規block d
作成に挑戦
c
b
a
悪しきノード
このノードは新
規block c’作
成に挑戦
block Cの事を
伝えない

想定されるエクリプス攻撃



現在想定している防衛策

- 隣接ノードが接続を受け付けている対象からの接続を受け付けない
- 広告とハンドシェイク時のaddrメッセージのネットワークアドレスの転送保存前のテスト
- 一定期間”block”が来ない場合全リンクをリフレッシュ
- ブートストラップノードの上記のケースでの活用

検証・評価

- 代数式、もしくはシミュレーションにより検証

- エクリプス攻撃による脅威と影響を
  - 攻撃に要するリソース(ノード数、時間)
  - 被害(長期のBlockchainの件数)

により評価

マイルストーン

5月~6月18日(修論題目変更申請書締め切り)

- サーベイの継続
- シミュレータの実装
- 検証
- 評価
- 執筆(Bitcoinに関する調査内容の章、関連研究)

6月中旬~7月2日 15:00 修士論文提出締め切り

- 執筆(評価)

まとめ

- 著名なデジタル通貨であるBitcoinの他ノードのネットワークアドレスの扱いに問題があり
- エクリプス攻撃に対して脆弱であり、通貨決済システムとしての価値と信頼を根本から損なう恐れ
- 当研究が指摘するエクリプス攻撃の手法に有効な防衛策を検討並びにその検証を行う