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

MAUI 2014/10/14

ARCH M2

bhangra

概要

当研究では:

- Bitcoin等の暗号通貨がネットワークにエクリプス攻撃に対して脆弱性を抱えている事を指摘し
- エクリプス攻撃のシミュレーションにより検証を行い
- 改善策の提案を行い、それによるエクリプス攻撃に対する効果をシミュレーションにより検証する

Bitcoin

- Bitcoinのデザインは分散取引記録、及び通り引きの承認の解決を中心に据えている
- 口座残高と取引の記録をネットワーク全体で合意しなければならず、Bitcoinはこれを”eventual consistency”[結果的な整合性]と呼ぶのが相応しい手法により解決している
- Bitcoinはグローバルな台帳を全ノードが持つ
- Bitcoinではネットワーク全体の決済記録を10分ほどで逐次追加されるBlockという情報で拡散、同期する

Block

- Blockの発見には報酬が伴い、攻撃者がBitcoinの決済記録の改変に必要な計算量を増大するよう、決済情報の更新、強化に参加するノードを増やしている

- 新規Blockが発見されたらネットワークに拡散

- 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と言われている

- Blockchain Fork発生後、当該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における新規ノードの接続

- Bitcoinでは新規ノードは、有志により運営されているDNSサーバを用いたDNSラウンドロビンによる接続

- 接続したノードに対する隣接ノードリストの問い合わせ命令

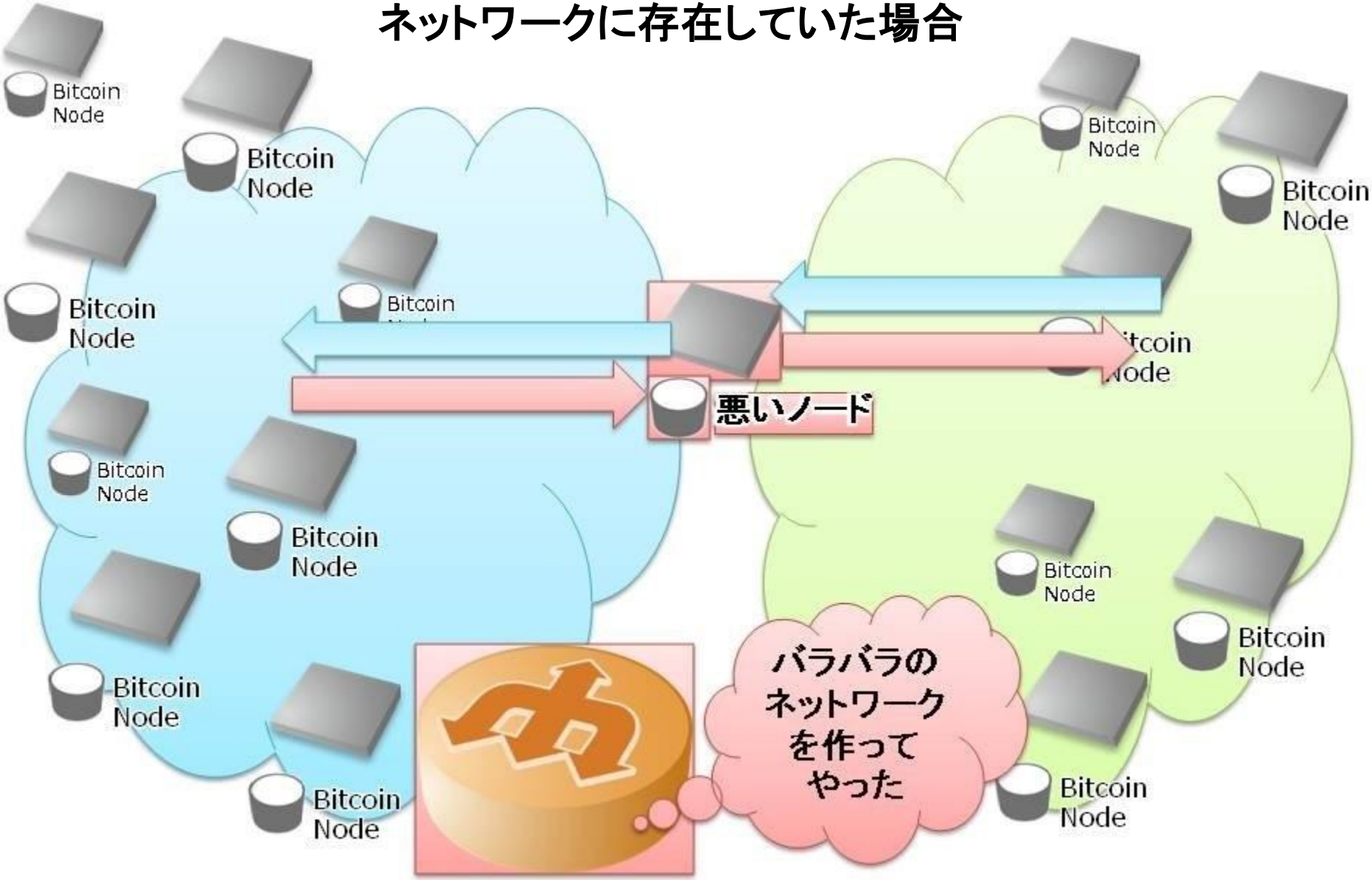
以上の2点で他ノードとの接続を行う

Bitcoinの想定しうる問題

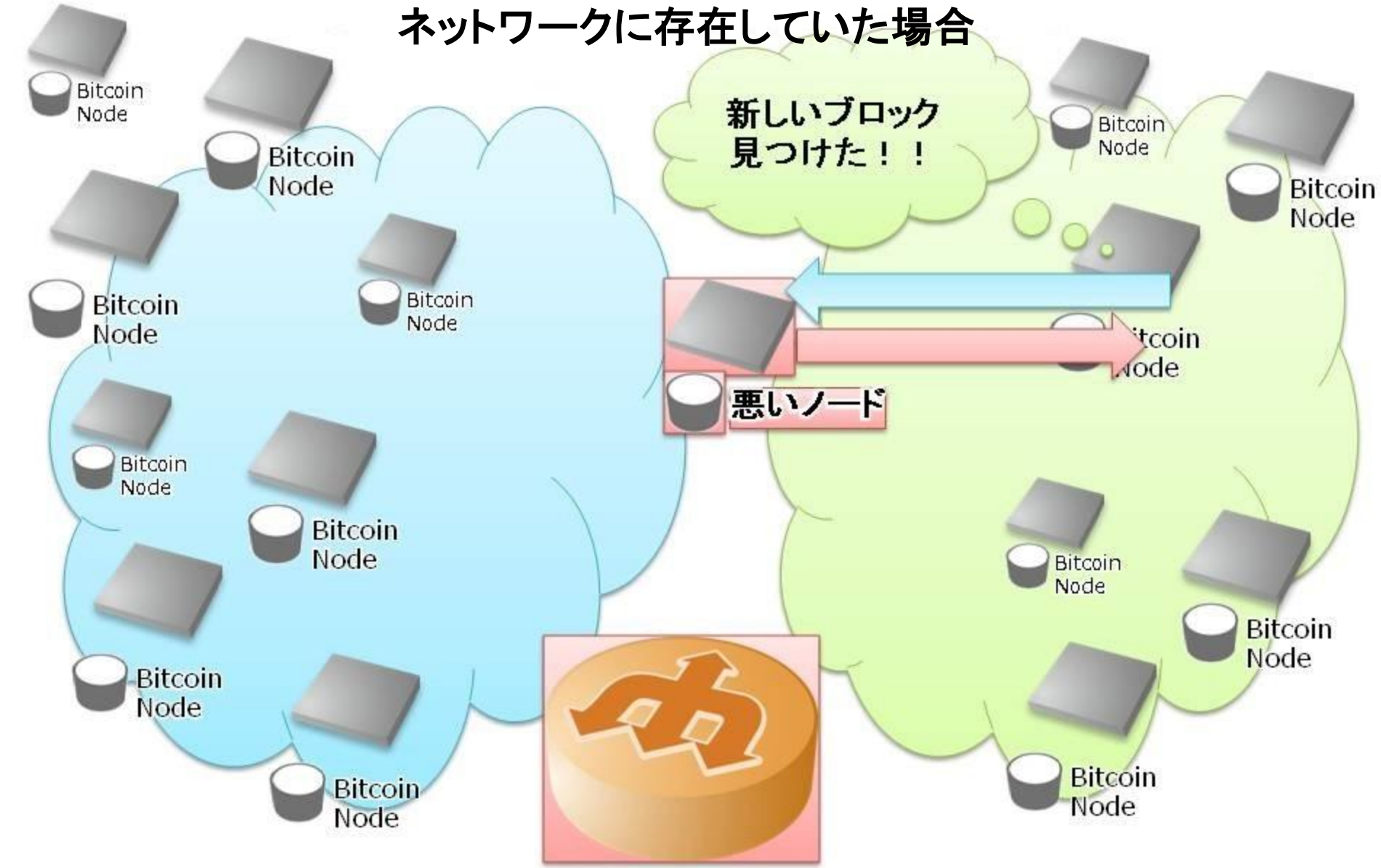
- Bitcoinネットワークでは、新規ノードのネットワークへの接続、ネットワークの形成が善意に乞うところが大きい

- 現用のBitcoinネットワーク実装ではネットワークエクリプス攻撃が有効な可能性があり、以下のような手法でブロックチェインフォークを引き起こし、台帳の内容をネットワーク全体で不一致させ、Bitcoinの通貨システムとしての信頼を覆す可能性がある

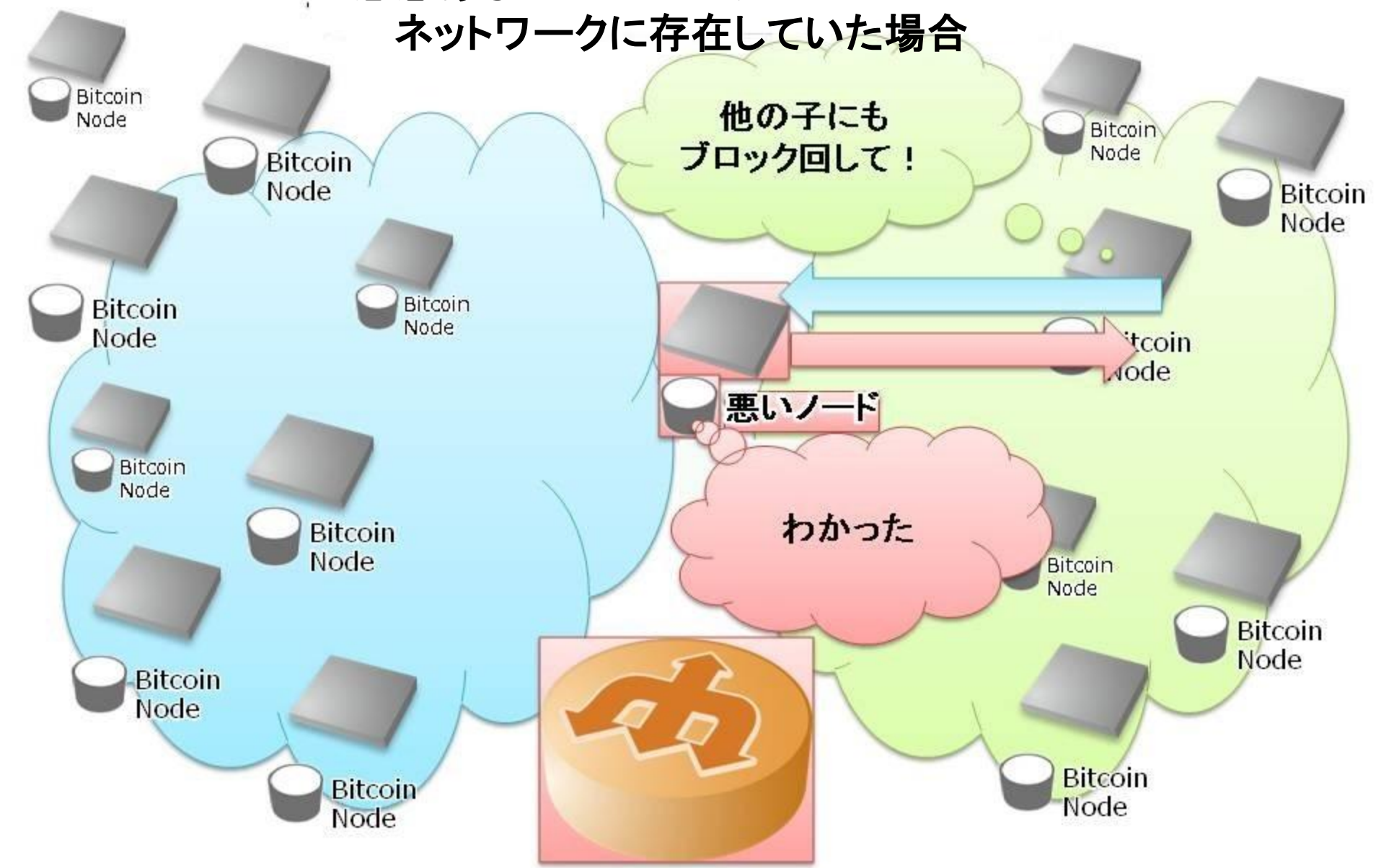
悪意あるノードとDNSサーバがBitcoinネットワークに存在していた場合



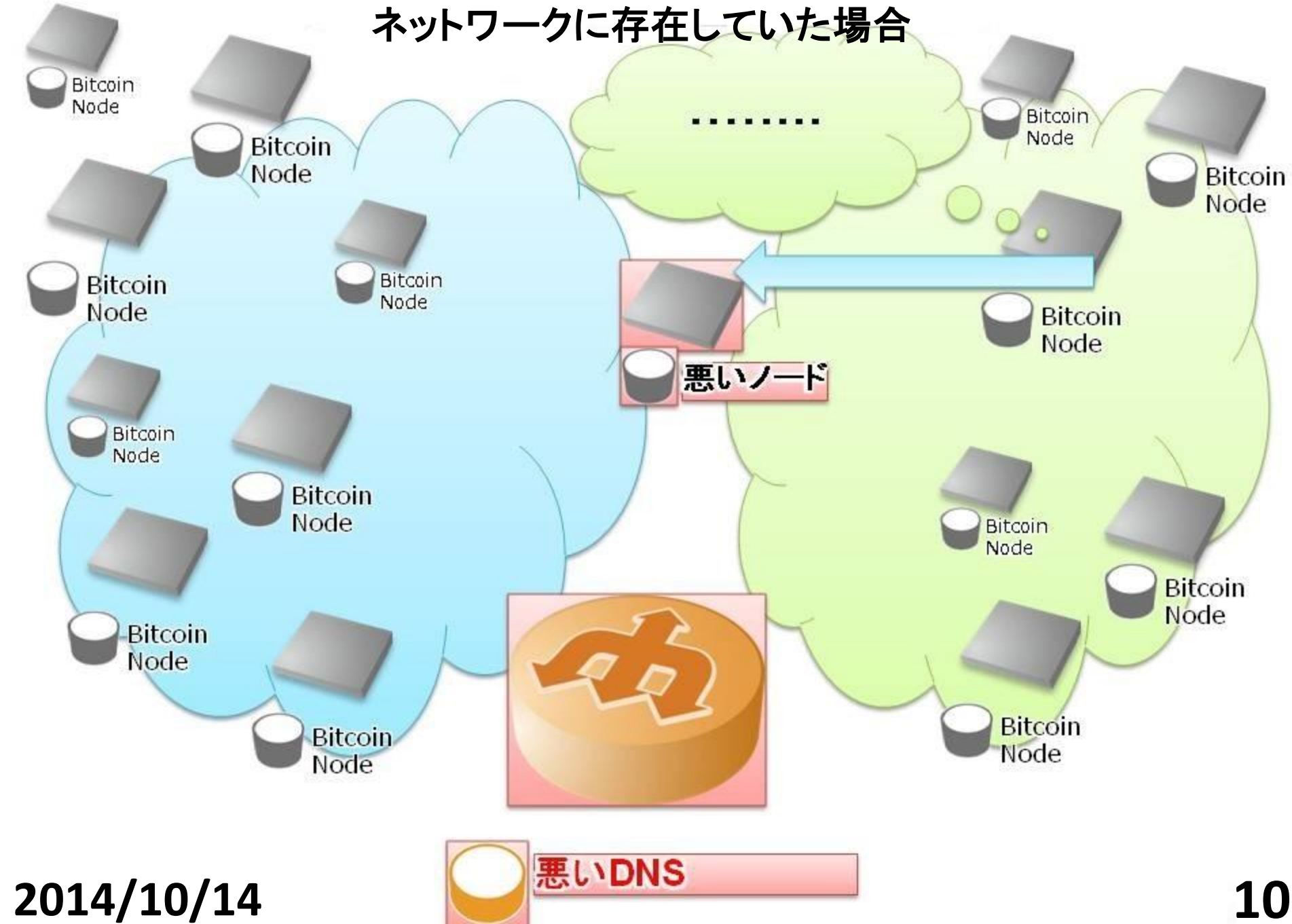
悪意あるノードとDNSサーバがBitcoinネットワークに存在していた場合



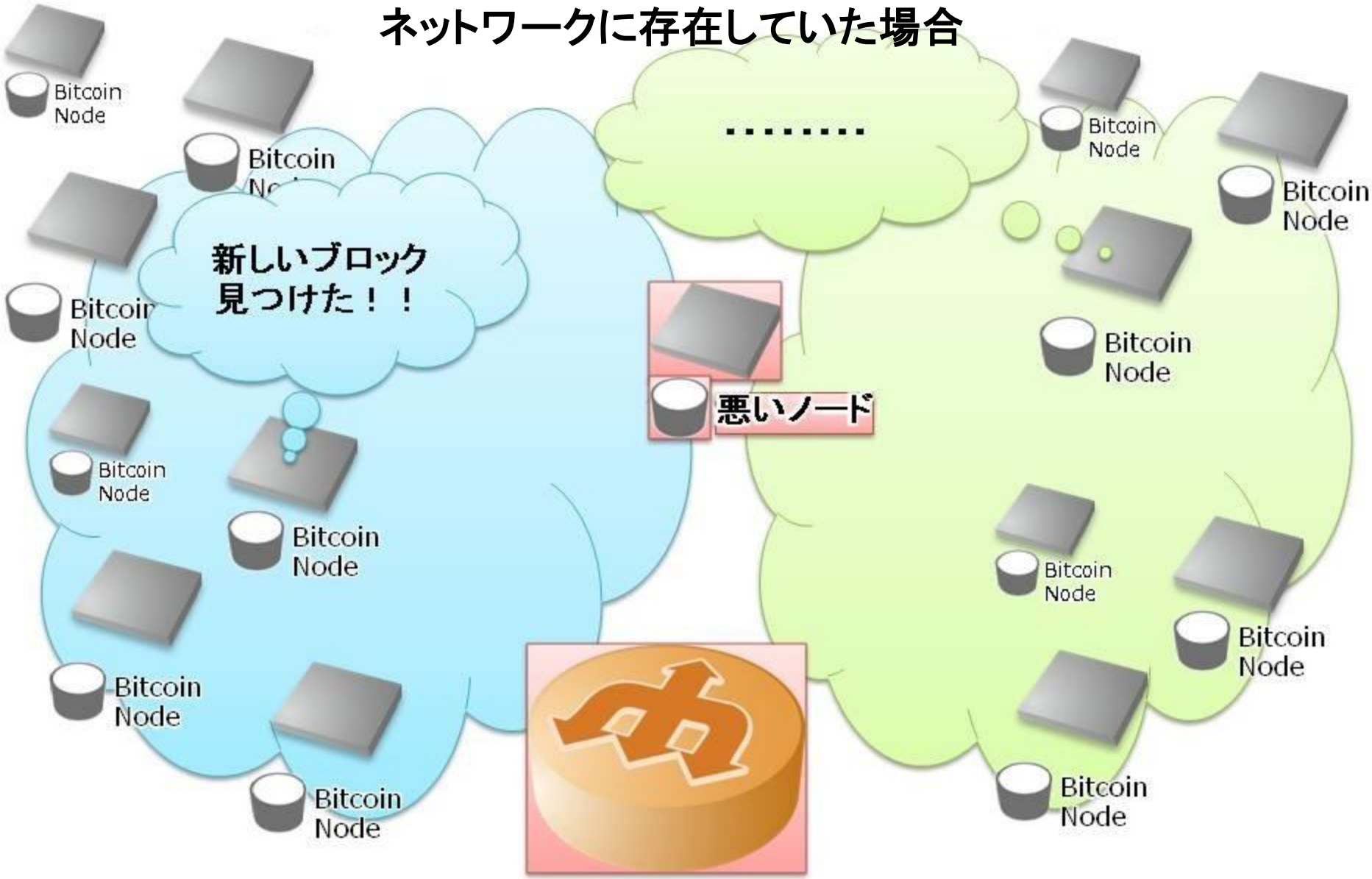
悪意あるノードとDNSサーバがBitcoinネットワークに存在していた場合



悪意あるノードとDNSサーバがBitcoinネットワークに存在していた場合



悪意あるノードとDNSサーバがBitcoinネットワークに存在していた場合



実験

- この様なネットワークエクリプス攻撃が実際に行いうるか、その影響の度合いをシミュレーションにて検証
- ネットワークを意図的にグループ化し分断するDNSサーバと悪意あるノードを設定
  - DNSサーバのみによるエクリプス攻撃の影響
  - ノードのみでエクリプス攻撃を敢行した際の影響
  - 両者の組み合わせによる影響

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、防衛手法を提案する事が当研究の目的である

TODO

- シミュレータの作成
- サーベイ
- 修論の執筆