第15回 地域間インタークラウドワークショップ
2019年 9月 4日(水)

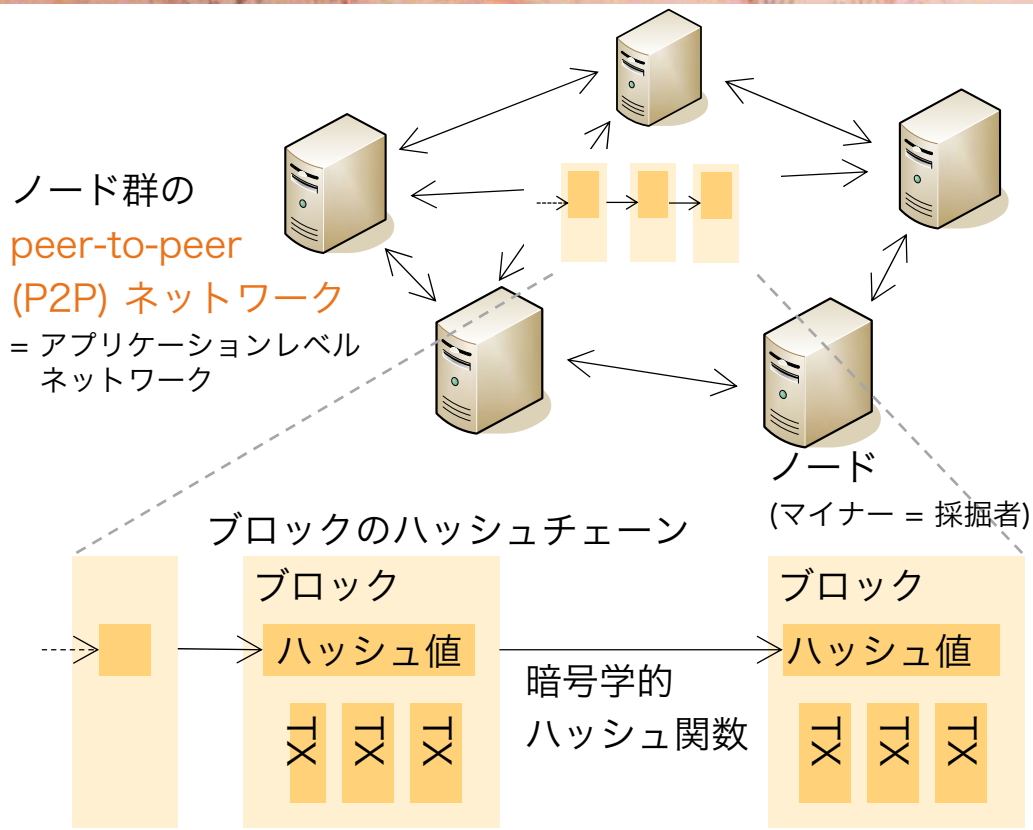
ブロックチェーン「ネットワーク」の研究

首藤 一幸
東京工業大学

SimBlock

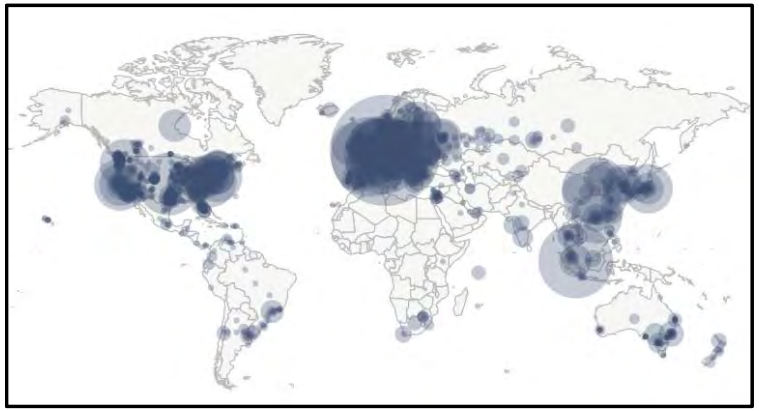
Tokyo Tech

ブロックチェーン



- トランザクション (TX) とブロックは全ノードにブロードキャストされる
- 全ノードが同一の台帳を保持する。
- ノード群はブロック生成競争をする
  → Proof of Work におけるマイニング

- 暗号通貨を支えている技術
  - Bitcoin の時価総額 20兆円
- 非集中 分散 / decentralized
- 期待されている応用
  - いわば時刻認証局, 公証役場
  - 流通履歴追跡、投票等の政治プロセス、組織の自動運営、…



Bitcoin ネットワーク　約 9,200ノード

出典：https://bitnodes.earn.com/

ブロックチェーンを支える技術

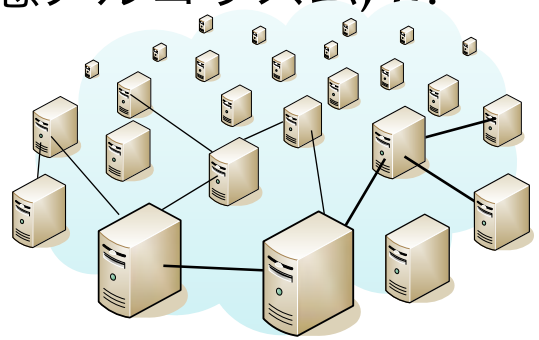
ブロックチェーンが達成したこと

- 不整合 (二重消費) 防止・改ざん困難
- 耐故障性
- 多数のノード群によるデータの承認

こちらをやる

- 暗号理論 / cryptography
  - 公開鍵暗号方式, それに基づく署名, 暗号学的ハッシュ関数, 乱数生成方式, …

- 分散システム / distributed systems
  - peer-to-peerネットワーク, flooding, 複製, 整合性, 分散合意アルゴリズム, …



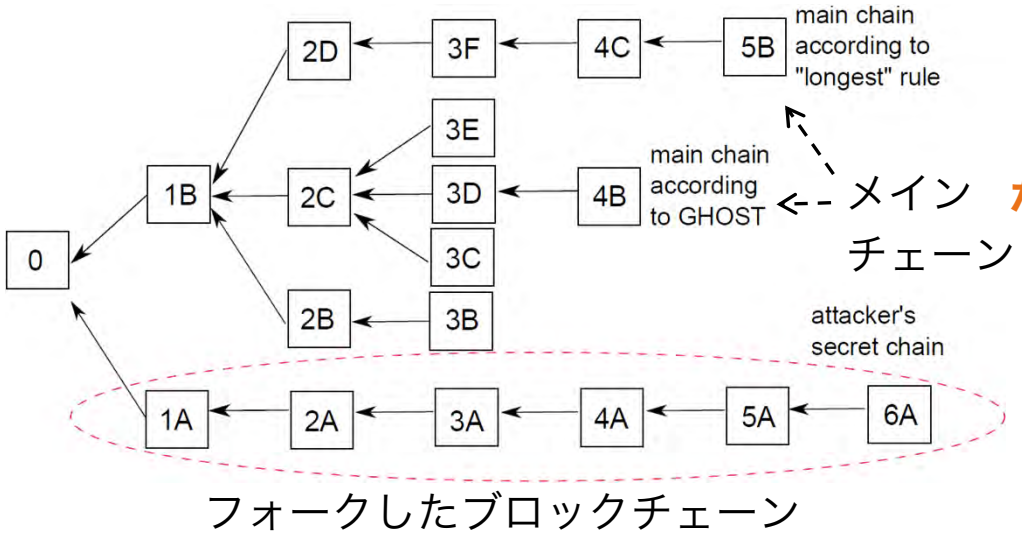
ブロックチェーンの課題

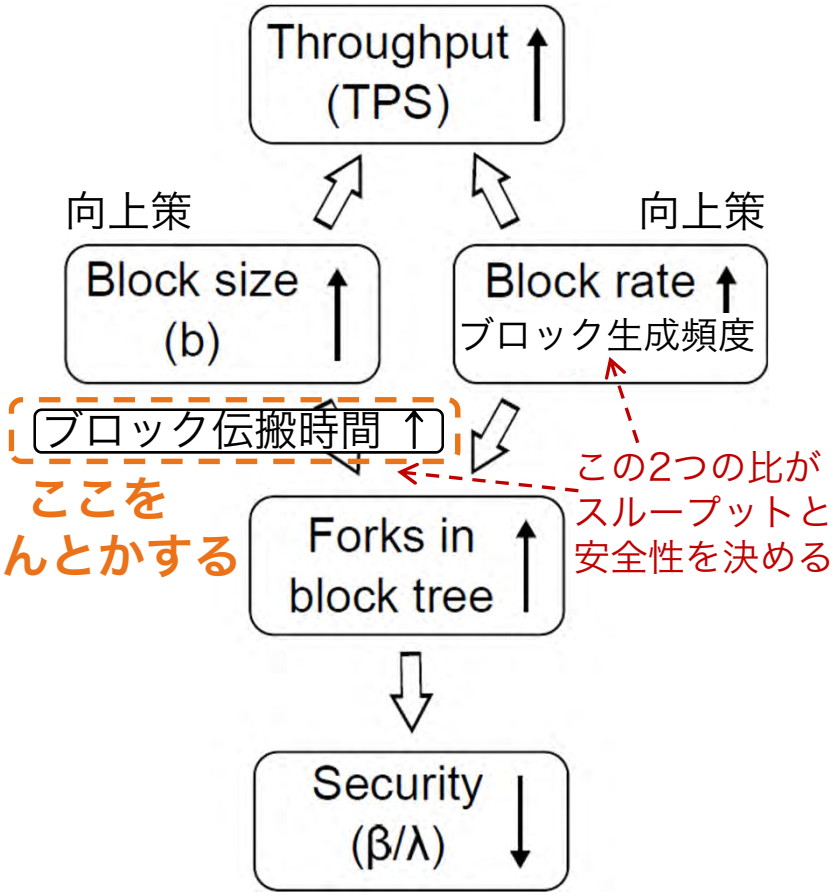
この講演のスコープ

- 承認までに要する時間
  - ブロック生成頻度 Bitcoin 10分, Ethereum 15秒
- 承認のスループット
  - Bitcoin 7件/秒, Ethereum (概算) ～300件/秒
  - PayPal 350件/秒, Visa 1,700件/秒
  - いわゆるスケーラビリティ問題 ➡ second layer, …
- 保持できるデータ量
  - 全ノードが同じデータを保持, > 200 GB
  - ➡ 間引く [Li 2019], DHTで分散 [Abe 2018], …
- 暗号通貨の運用が必要
  - 暗号通貨が崩れると応用も総崩れ
  - ➡ 移植性・移送 [Shudo 2018], …
- 他にもいろいろ面白い問題が

スループット向上と安全性の相克

- スループット向上策が安全性の低下を招く
  - メインチェーン以外でのブロック生成が増えると、攻撃が容易に。
    例：51% 攻撃による TX 無効化
  - ブロックの生成頻度と伝搬時間の比
    ➡ フォーク発生率 ➡ 安全性



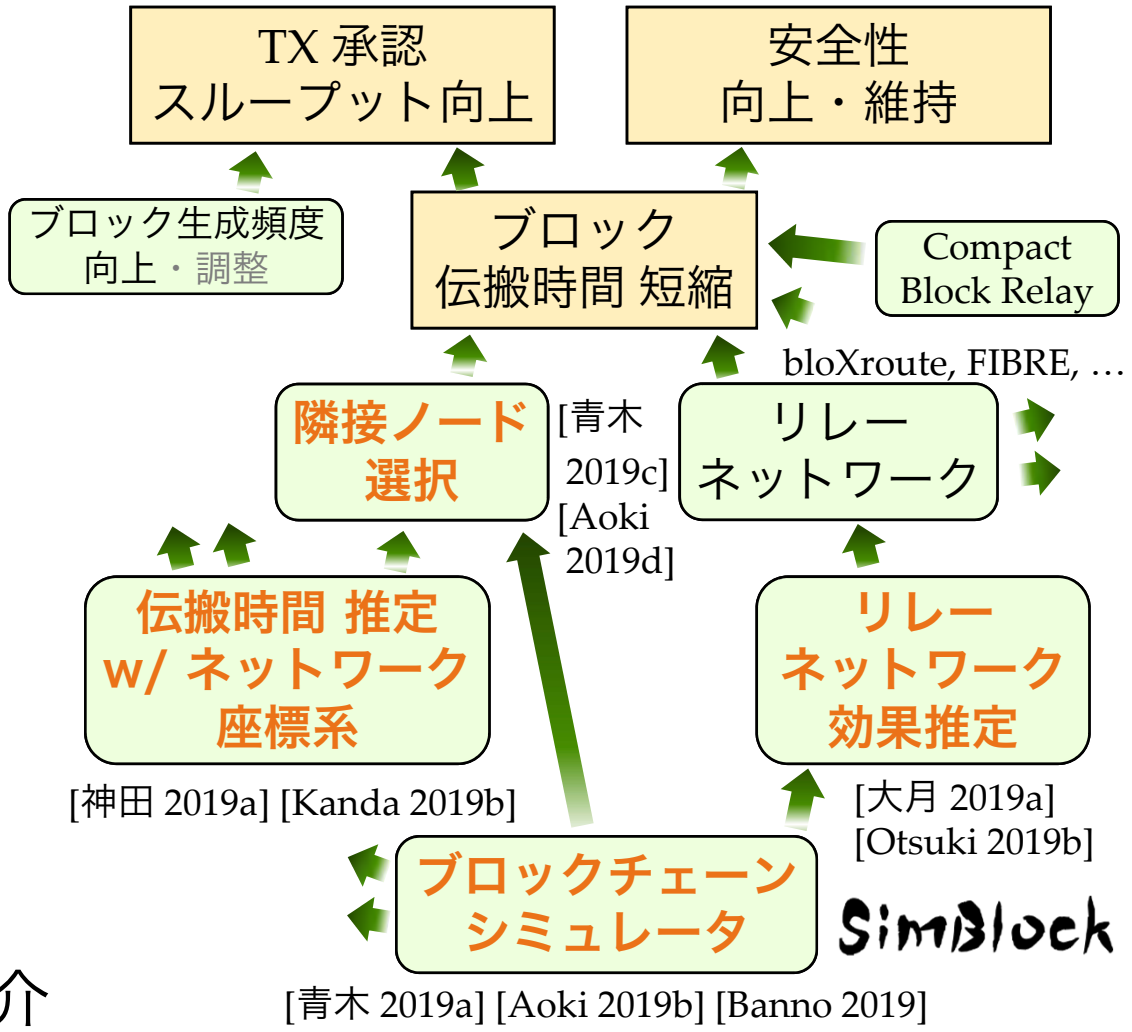


“Secure High-Rate Transaction Processing in Bitcoin”, FC’15, 2015 の図

性能と安全性の両立に向けて

- 伝搬時間 推定 with ネットワーク座標系
- ブロックチェーン シミュレータ
- 隣接ノード選択
- リレーネットワーク 効果推定

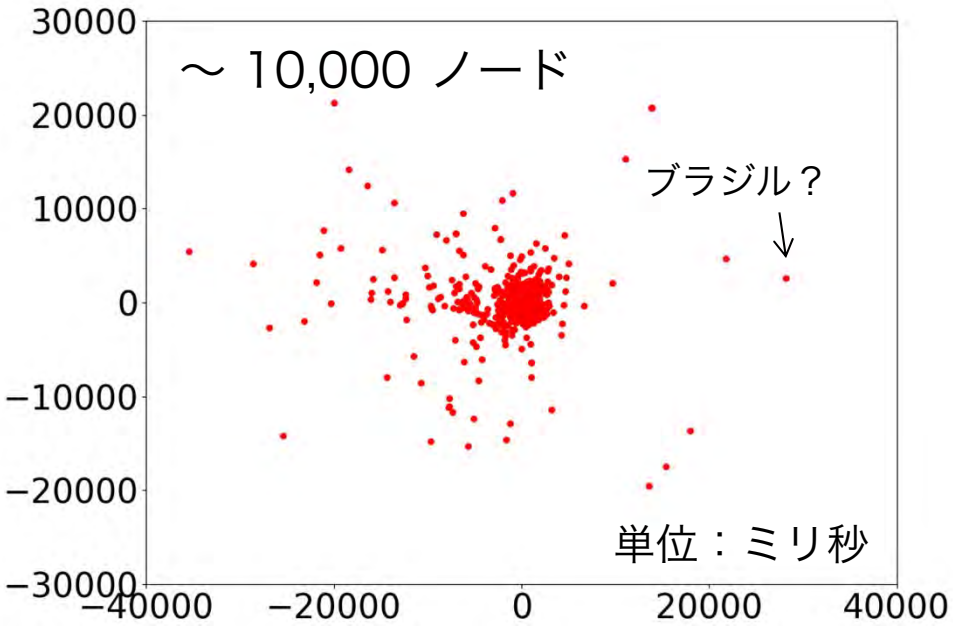
順に紹介



伝搬時間 推定 with ネットワーク座標系

[神田 2019a]
[Kanda 2019b]

- ネットワーク座標系 [Dabek 2004] [Chen 2007]
  - を適用して、ノード間伝搬時間を推定
  - n次元座標系＋バネモデルでの位置決め



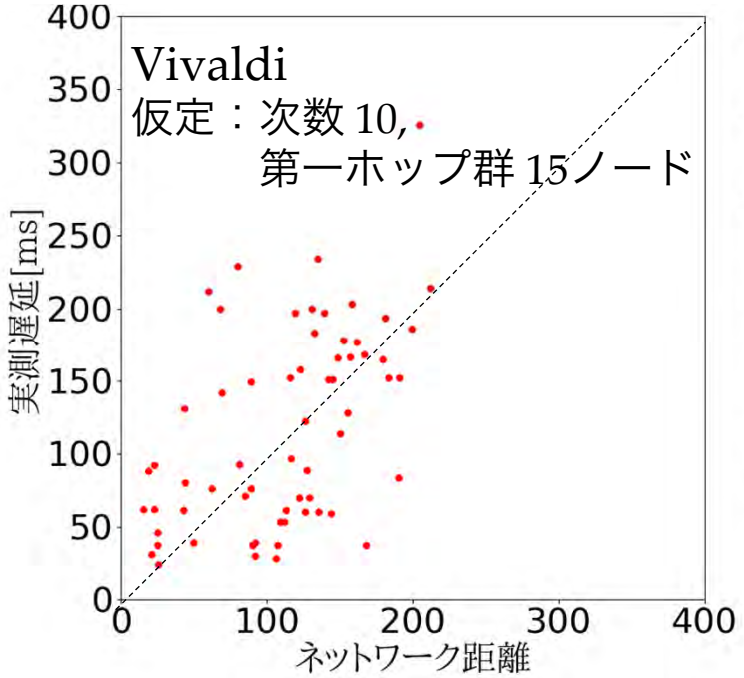
- 狙い
  - 伝搬高速化手法の指針
  - 隣接ノード選択の指針
- 現状と今後
  - 精度の向上
  - そのための
    トポロジ取得と推定

- ただ…

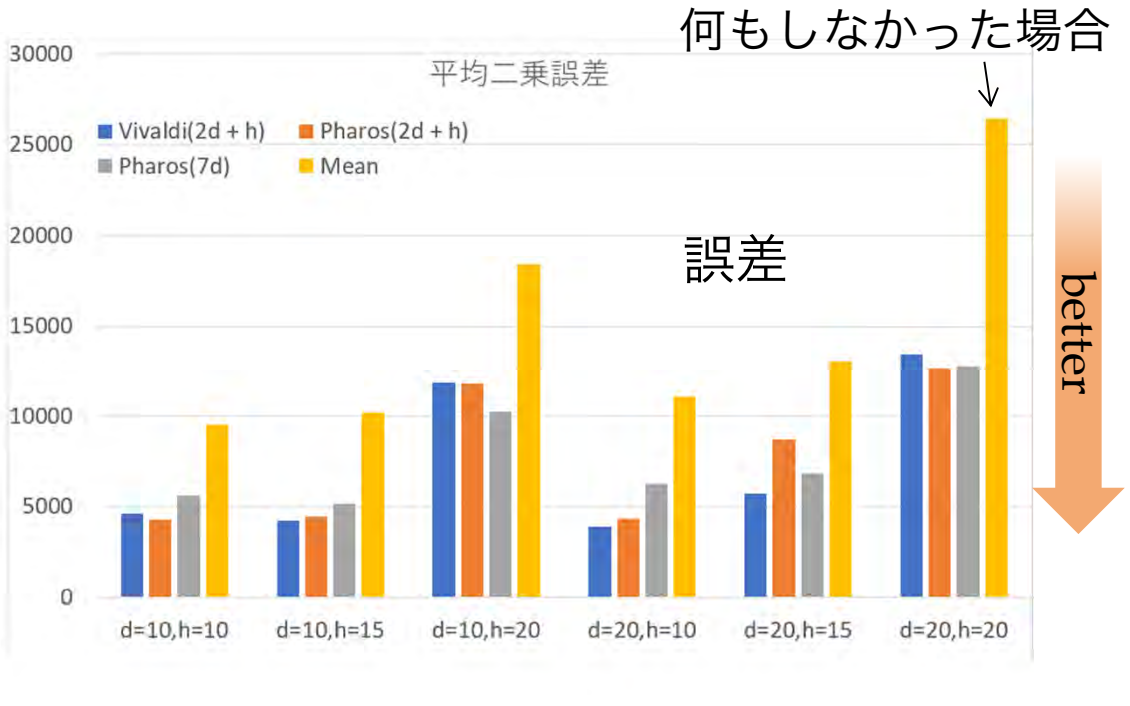
伝搬時間 推定 with ネットワーク座標系

[神田 2019a]
[Kanda 2019b]

- 精度は ほどほど



推定値と実測値が
あまり一致していない？



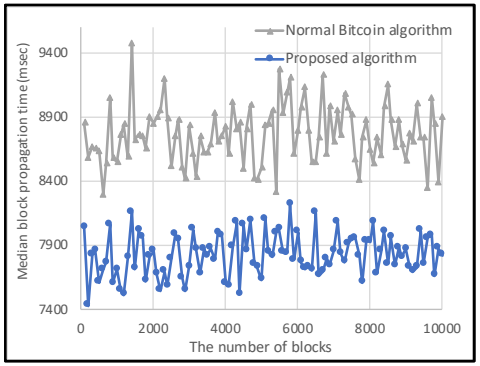
効果がまったくないわけでもない

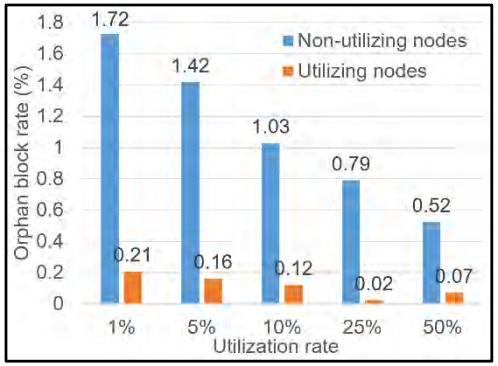
- トポロジが不明なのが、ボトルネック
  - cf. “TxProbe: Discovering Bitcoin’s Network Topology …”, FC’19, 2019

シミュレータ SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019]

- (パブリック) ブロックチェーン「ネットワーク」のシミュレータ
  - 2019年 6月 27日(木) 公開・プレスリリース
  - インターネット上のノード間でのブロック / トランザクション伝搬、Proof of Work のマイニングをシミュレート
    - 離散イベントシミュレーション
  - 可視化ツール
  - 現在、Bitcoin, Litecoin, Dogecoin のパラメータを提供
  - 研究の例：

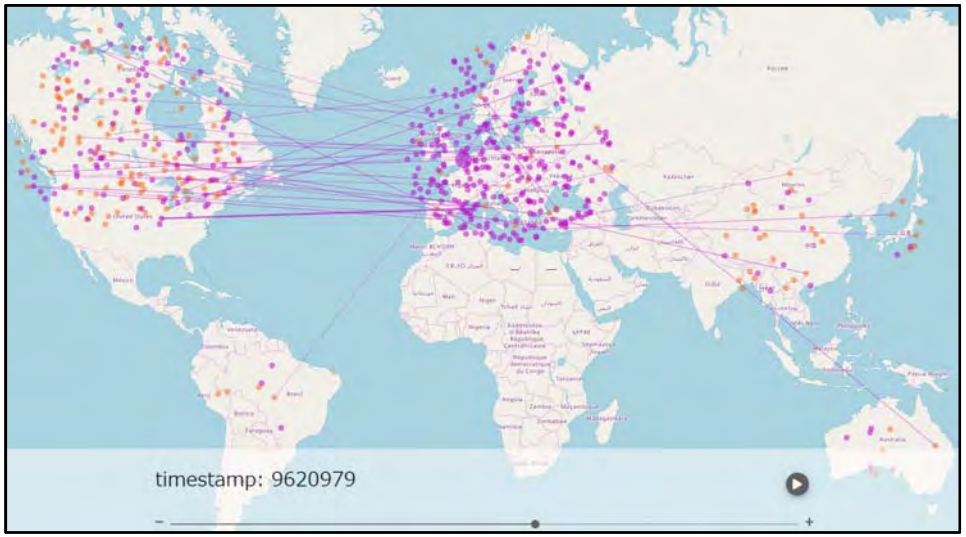




隣接ノード選択　リレーネットワーク 効果推定

シミュレータ SimBlock

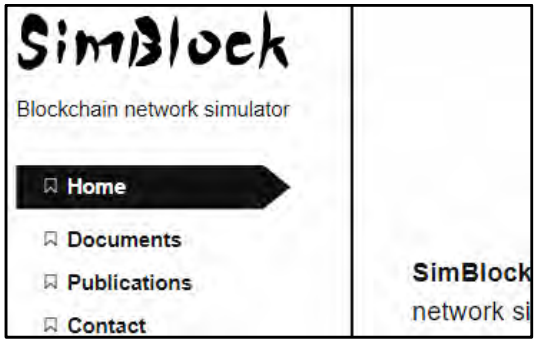
[青木 2019a] [Aoki 2019b] [Banno 2019]



Visualizer

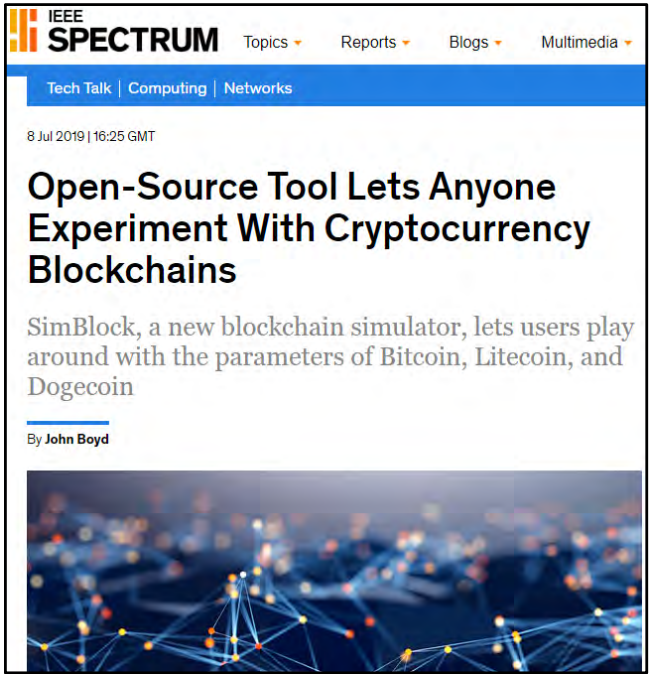
縮小 Bitcoin ネットワーク,
600 ノード

ウェブ
サイト



IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

IEEE Spectrum
記事



隣接ノード選択

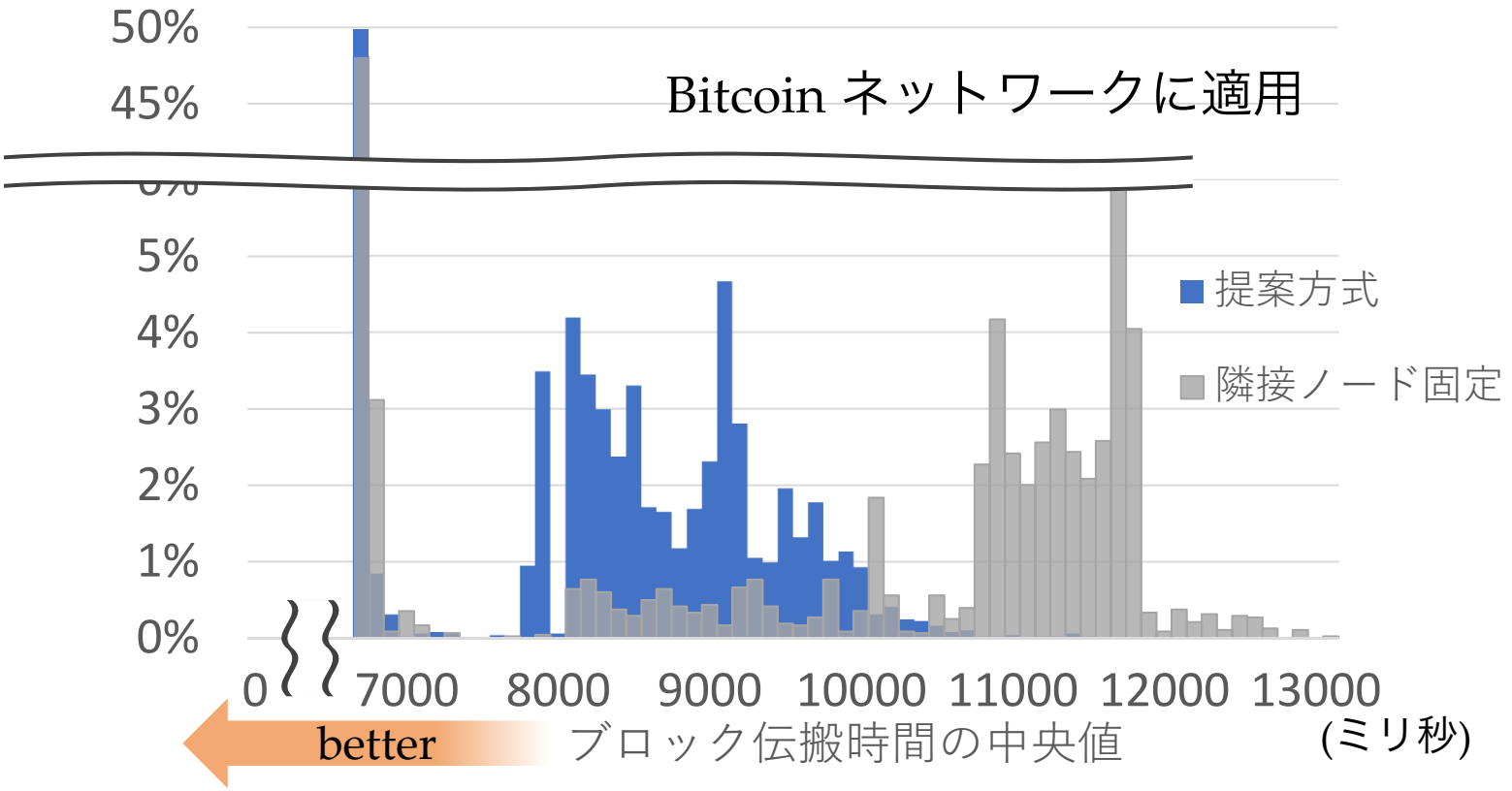
[青木 2019c] [Aoki 2019d]

- 速く通信できる相手と優先的につながる
- peer-to-peer 分野でメジャーな手法
  - 例えば DHT では proximity (近接性) {ID, neighbor, route} selection
  - 僕らもやった：DHT での proximity neighbor selection [Miyao 2013]
  - 実験手段がなかったので、シミュレータを作った
- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

隣接ノード選択

[青木 2019c] [Aoki 2019d]

- そこそこ縮まった
  - 伝搬に時間がかかったブロック群で、11.5 秒 → 8.5 秒 くらい

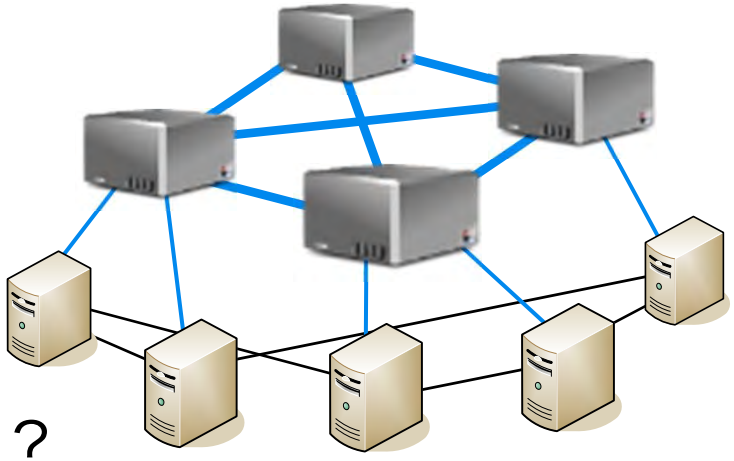


- 課題: Compact Block Relayの考慮, インターネットのパラメータ更新

リレーネットワーク 効果推定

[大月 2019a] [Otsuki 2019b]

- リレーネットワーク
  - ブロック高速配信ネットワーク
  - bloXroute (2018), FIBRE (2016), Falcon (2016), BFRN (2014), …
  - bloXroute: Falcon をやっていた Cornell U. の人達がビジネスとして開始



リレー
ネットワーク

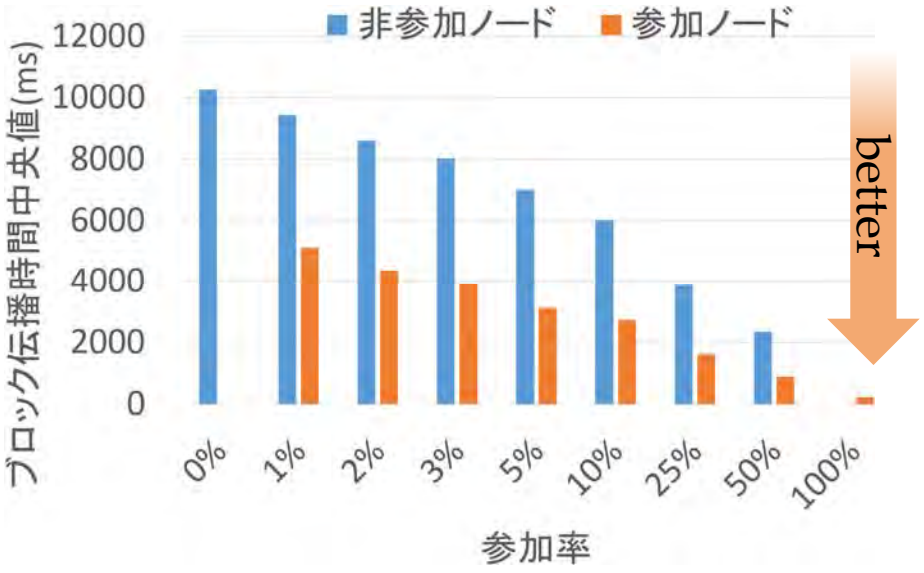
通常の
ブロックチェーン
ネットワーク

- 効果は？
  - 孤立ブロックはどのくらい減る？
  - ブロックを早く受け取れるのだから、マイニング成功率が上がる？

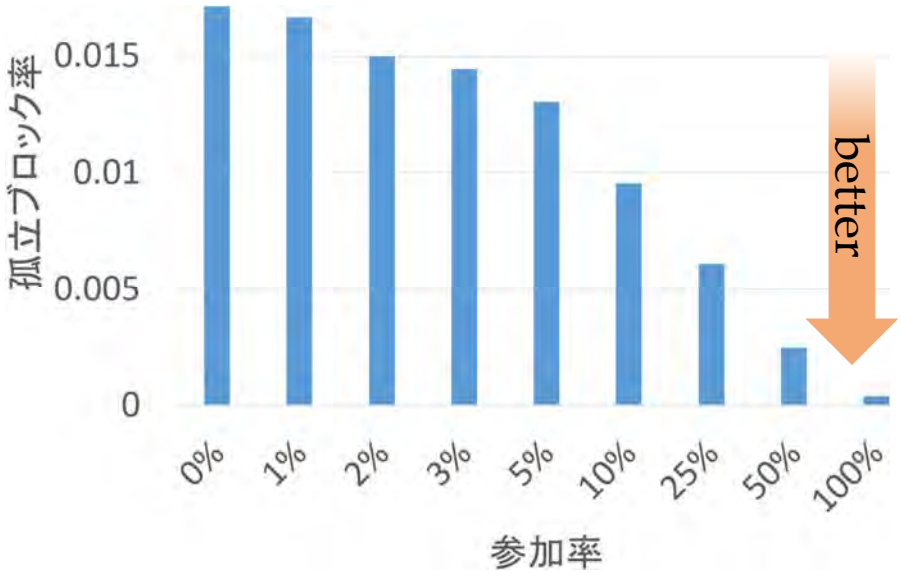
リレーネットワーク 効果推定

[大月 2019a] [Otsuki 2019b]

- SimBlock 上の Bitcoin ネットワークで実験
  シミュレータ
- ネットワーク レベル：



伝搬が速くなった！



孤立ブロックが減った！

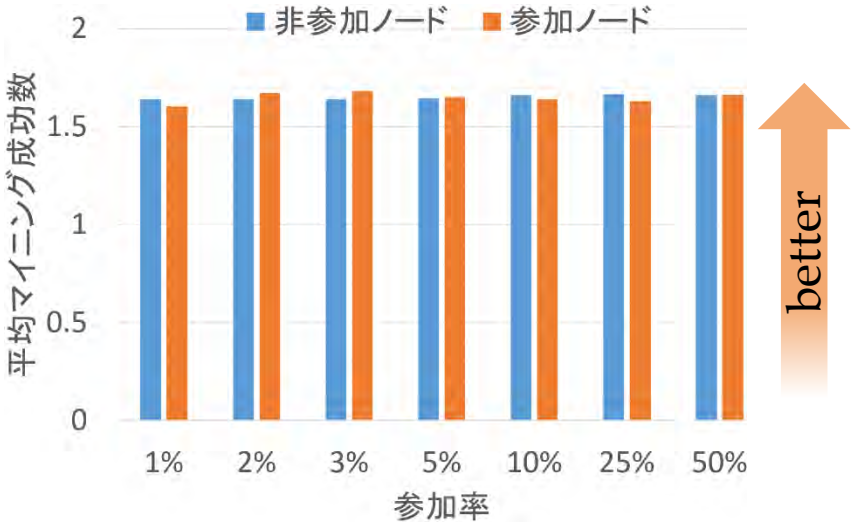
↑
フォークによって発生した、
メインチェーンから外れたブロック

- では、ノード レベルでは？

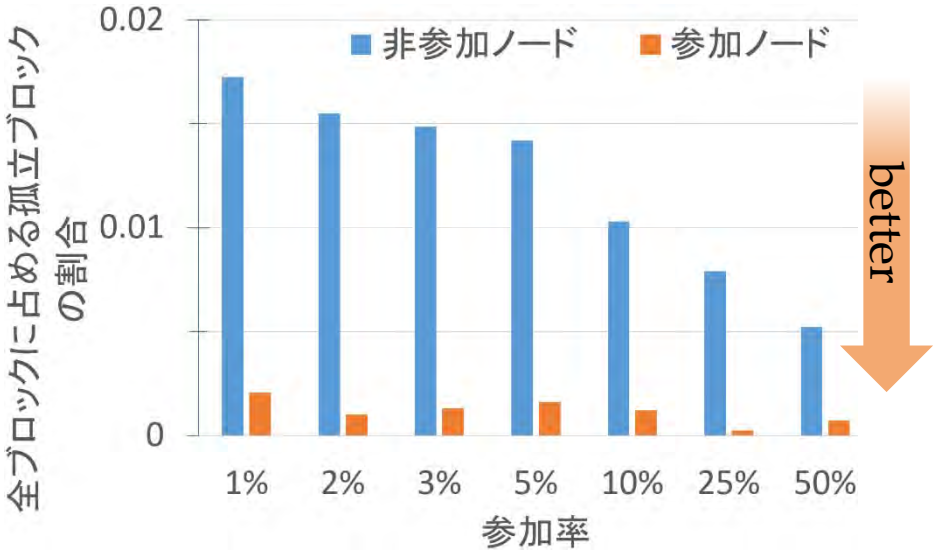
リレーネットワーク 効果推定

[大月 2019a] [Otsuki 2019b]

- ノード レベル：



マイニング成功率は
変わらないが…



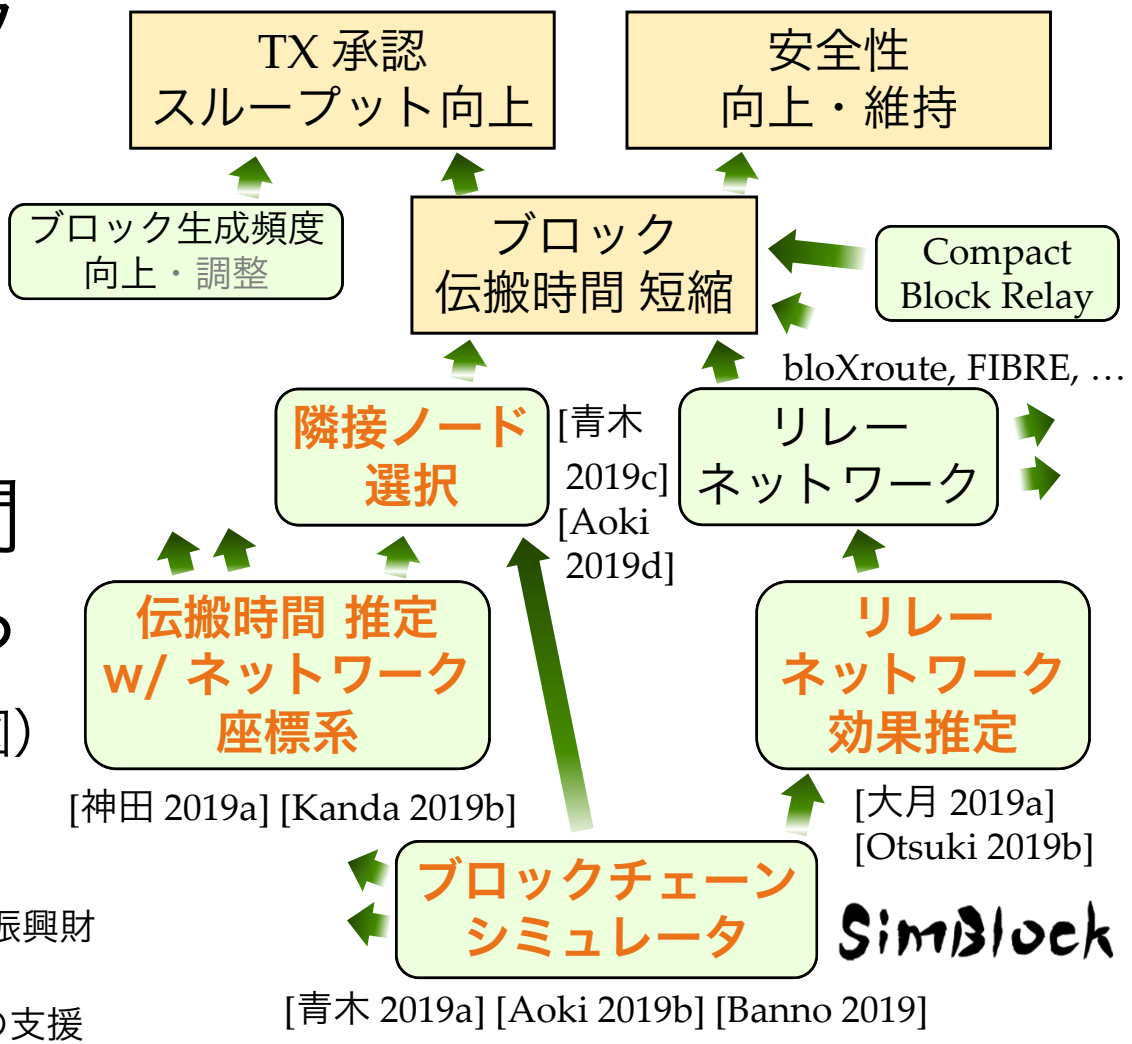
生成したブロックが
孤立ブロックになって
しまう率が低下！

➡ マイニング報酬 増加

これがリレーネットワークの効能

ブロックチェーン「ネットワーク」の研究

- 課題：トランザクション承認
  - までの時間
  - スループット
- ブロック伝搬時間短縮を狙っていろいろやってる（右図）



- 謝辞
  - 本研究は（公財）セコム科学技術振興財団の支援を受けたものです。
  - 伝搬時間推定の研究はカウラ(株)の支援を受けたものです。

論文

- 私達
  - [Shudo 2018] “Towards Application Portability on Blockchains“, IEEE HotICN 2018, 2018年 8月
  - [神田 2019a] “ビットコインネットワーク上でのデータ伝搬遅延推定”, 信学技報, Vol.118, No.481, IA2018-77, pp.317-322, 2019年 3月
  - [Kanda 2019b] “Estimation of Data Propagation Time on the Bitcoin Network”, AINTEC 2019, 2019年 8月
  - [大月 2019a] “Bitcoinネットワークに対するリレーネットワークの影響”, 信学技報, Vol.118, No.481, IA2018-76, pp.309-316, 2019年 3月
  - [Otsuki 2019b] “Effects of a Simple Relay Network on the Bitcoin Network”, AINTEC 2019, 2019年 8月
  - [青木 2019a] “SimBlock: ブロックチェーンネットワークシミュレータ”, 信学技報, Vol.118, No.481, IA2018-70, pp.219-224, 2019年 3月
  - [Aoki 2019b] “SimBlock: A Blockchain Network Simulator“, CryBlock 2019, 2019年 4月
  - [Banno 2019] “Simulating a Blockchain Network with SimBlock“, IEEE ICBC 2019, pp.3-4, 2019年 5月
  - [青木 2019c] “ブロックチェーンネットワークにおける隣接ノード選択”, 信学技報, Vol.118, No.481, IA2018-71, pp.225-232, 2019年 3月
  - [Aoki 2019d] “Proximity Neighbor Selection in Blockchain Networks“, IEEE Blockchain 2019, 2019年 7月
  - [Miyao 2013] “A Method for Designing Proximity-aware Routing Algorithms for Structured Overlays”, IEEE ISCC’13, 2013年 7月
- 他
  - [Li 2019] “Downsampling Blockchain Algorithm”, CryBlock 2019, 2019年 4月
  - [Abe 2018] “Mitigating Bitcoin Node Storage Size By DHT”, AINTEC 2018, 2018年 11月
  - “Secure High-Rate Transaction Processing in Bitcoin”, FC’15, 2015年 1月
  - [Dabek 2004] “Vivaldi: A Decentralized Network Coordinate System”, ACM SIGCOMM 2004, 2004年 9月
  - [Chen 2007] “Pharos: A Decentralized and Hierarchical Network Coordinate System for Internet Distance Prediction”, IEEE GLOBECOM 2007, 2007年 12月
  - “TxProbe: Discovering Bitcoin’s Network Topology Using Orphan Transactions”, FC’19, 2019年 2月