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 bit.ly/NS-202106-shudo

Tokyo Tech

首藤 一幸 (47)

しゅどう　かずゆき

1996　早稲田大学 修士課程

1998　早稲田大学 博士課程

2001　産総研　**国研**

2006　ウタゴエ(株)

スタートアップ

2008/12 東工大　**大学**

2009/ 5 未踏 PM

2018/11 (株)アーリーワークス 顧問

2018/11 (公財) GMOインターネット財団 理事

2019/ 1 Miraise (シード特化ファンド) メンター

魔法のようなソフト

Java スレッド移送システム MOBA

Java Just-in-Time コンパイラ shuJIT

17,000ダウンロード, 商用

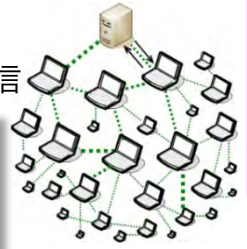
P2P の基盤ソフト Overlay Weaver

26,000ダウンロード, 15ヶ国

41ヶ国 673台以上で動作 (データベース)

P2P ライブ配信ソフト UG Live

未踏スパクリ × 2人, 商用化, 1万数千人に同時配信



書籍 Binary Hacks

1万数千部, ネタ100個中 10個執筆

大規模分散システム

P2P のアルゴリズム, 2009 ～

構造化オーバレイ / DHT の統一フレームワーク

分散データベース, 2009 ～

読み書き性能両立, Causal consistency, NVRAM / SCM

分散システムのシミュレーション, 2011 ～

1億ノード / 10台, 既存手法の20倍の性能, Apache Spark 上

ソーシャルネットワーク解析, 2013 ～

非集中 分散 機械学習, 2016 ～

ブロックチェーン, 2016 ～

シミュレータ SimBlock, 性能と安全性, 新アーキ

2021年 6月

講演の概要

- ブロックチェーンの起源・価値
  - 暗号通貨 Bitcoin
  - 非集中に二重使用を防止 → trustless
- 首藤研での研究
  - 性能
  - ツール
  - セキュリティ
  - 公平性
  - 分権化
- まとめ

ブロックチェーンの
起源・価値

- 暗号通貨 Bitcoin
- 非集中に二重使用を防止 → trustless

暗号通貨　または仮想通貨, 暗号資産

cryptocurrency　　crypto asset

- デジタルなお金は、いろいろある。
  - Suica, PASMO, PayPay, ○○ポイント, …

3,000 種類以上ある

- 暗号通貨：Bitcoin (BTC), Ethereum (ETC), Ripple (XRP), …
  - Bitcoin に端を発する、非集中的 (後述) なもの
  - Bitcoin 時価総額 数十兆円　「通貨」になりたいが現状「資産」

暗号通貨の起源

- 2008年の論文

  ネットで見つかる。
  和訳もある：
  https://coincheck.blog/292
  読むのもいいのでは？

Bitcoin: A Peer-to-Peer Electronic Cash System

ビットコイン: peer-to-peer 電子現金 システム

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

- 2009年 1月のメール

Bitcoin v0.1 released

Satoshi Nakamoto satoshi at vistomail.com

Thu Jan 8 14:27:40 EST 2009

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Satoshi Nakamoto
が誰なのかは、
今日に至るまで不明

Bitcoin の非集中 分散システム

- インターネット上に約 1万ノード (サーバ)
  - インターネット側からは通信できないノードを含めると、数万

GLOBAL BITCOIN NODES DISTRIBUTION

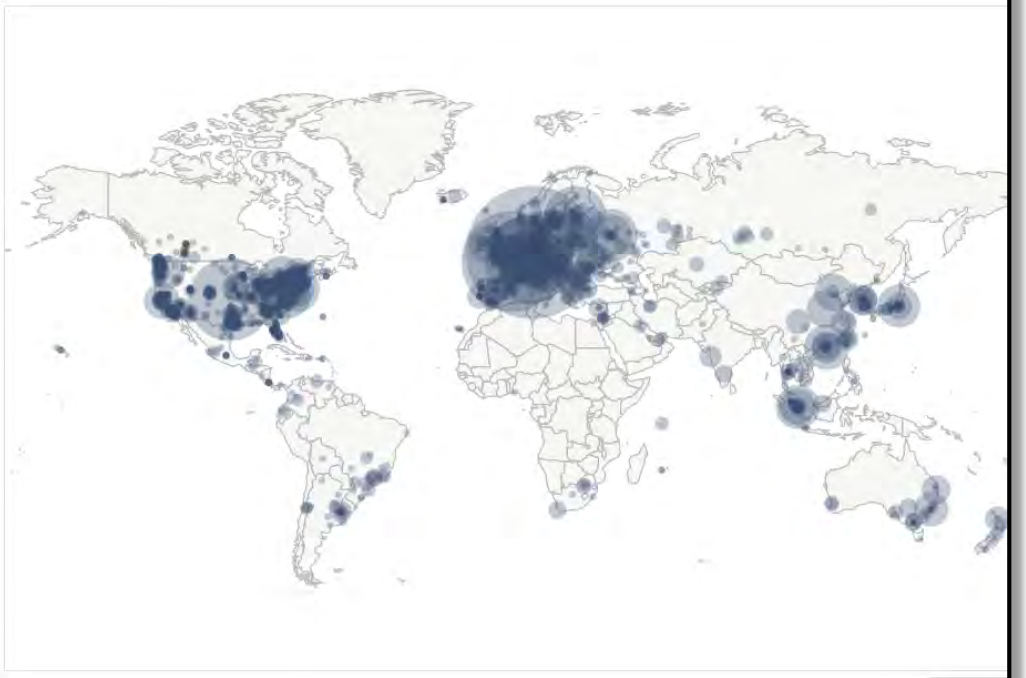
Reachable nodes as of Wed Jun 23 2021 18:32:02 GMT+0900 (日本標準時).

9812 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2363 (24.08%)
2	United States	1748 (17.81%)
3	Germany	1689 (17.21%)
4	France	568 (5.79%)
5	Netherlands	421 (4.29%)
6	Canada	311 (3.17%)
7	United Kingdom	267 (2.72%)
8	Russian Federation	228 (2.32%)
9	Finland	168 (1.71%)
10	China	152 (1.55%)

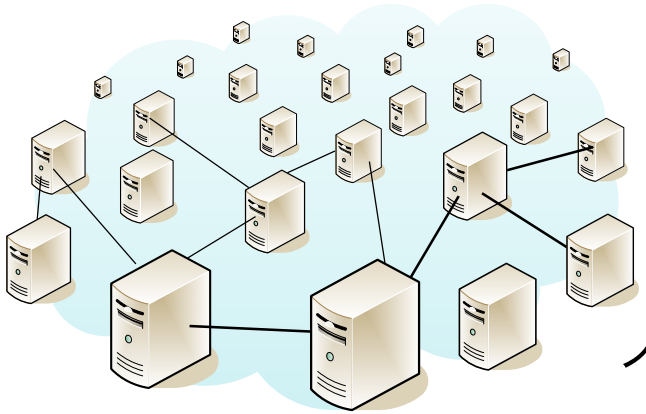


https://bitnodes.io/ より

- 非集中 → 一部壊れても全体は動作し続ける

トラストレス / trustless

- 非集中 / decentralized



ピア / peer
ノード / node

非集中 分散システム (peer-to-peer)

- 誰かを信用する必要がない → 「トラストレス **trustless**」
  - 政府, 銀行, 企業, … 等を信用する必要がない。
  - 実際は、ノードのうち例えば 2/3 は悪意のないノード (運用者) である必要がある。

ブロックチェーン

- 暗号通貨 Bitcoin が提供した価値
  - 非集中 (→ トラストレス) に
  - 二重使用を防止
    - 整合性 を保つ
    - 改ざん困難性
- … これは、通貨に限らず他に応用できるのでは？

ブロックチェーン または
Distributed Ledger Technology (**DLT**) / 分散台帳技術

「ブロックチェーン」は特定のデータ構造を指す語なので、
それを嫌って、DLT と呼ぶ人も多い。

ブロックチェーンの価値

- 非集中
  decentralized
  派生 → **トラストレス**
  trustless
  派生 → **耐故障性**
  fault tolerant
  非集中に加えて
  - 複製
  - 悪意あるノードに耐えるトランザクション承認方式

二重使用の防止

- **整合性** を保つ
  consistent
  派生 → **トレーサビリティ**
  traceability
  整合性確認のために
  (全) 履歴を残すので
- **改ざん困難性**
  unalterable, tamper proof, …

首藤研での研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

首藤研での 研究

- 「ツール」「性能」から「セキュリティ」「分権化」「公平性」へ

セキュリティ [Nagayama 2019]

- selfish mining 攻撃への耐性評価
- Erebus 攻撃対策の性能への影響 [高山 2020b]
- PoS への攻撃手法と耐性調査 [大月 2021a]

相互に影響

性能 含 実時間性・スケールアウト性

- 伝搬時間 推定 [神田 2019a] [Kanda 2019b]
- 隣接ノード選択 [青木 2019c] [Aoki 2019d]
- プロトコルの効果推定 [永山 2020a] [Nagayama 2020b]
- リレーネットワークの影響推定 [大月 2020a] [Otsuki 2020b]
- ブロードキャスト木の適用 [北川 2021a] [北川 2021b]

研究手段を提供

ツール

- シミュレータ SimBlock [青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

研究手段を提供

分権化 / decentralization [高山 2020a]

- 中央集権の度合い評価
- 新アーキテクチャ [Nagayama 2020a]

公平性 / fairness

- 指標と向上手法 [神田 2020a] [Kanda 2020b]

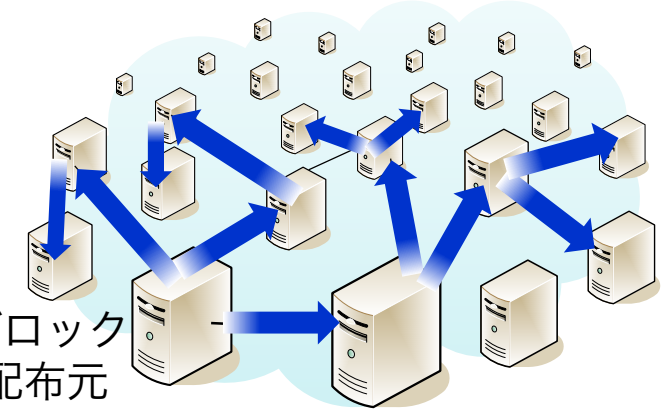
Ethereum 開発者会議 (Devcon 5) での発表 [Nagayama 2019]

性能 の研究

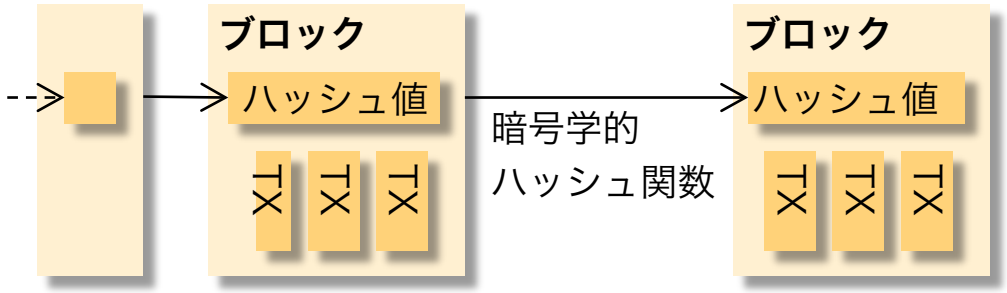
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

パブリック
ブロックチェーンの性能

- 性能：トランザクション (取引, TX) / 秒 = TPS
  - TX の例：Aさんから Bさんに 1 BTC 送金
  - – 既存　VISA (クレジットカード) 1,700 TPS, PayPal 平均 320 TPS
  - – 暗号通貨　Bitcoin 7 → 27 TPS, Ethereum 15 TPS 前後　**圧倒的に不足**
- 性能向上には、ノード (サーバ) 間での
  データ伝搬の高速化が欠かせない。　理屈は次ページ



ノード (サーバ) のネットワーク

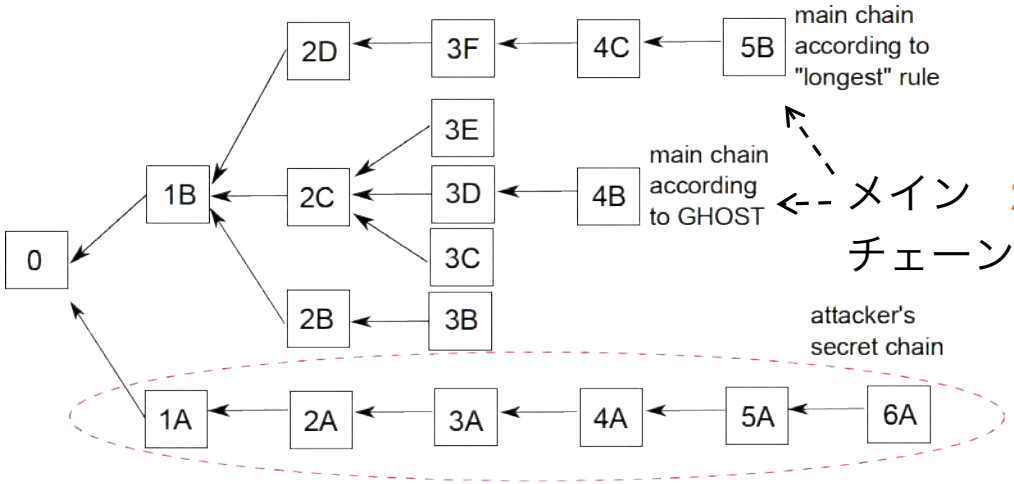


ブロックチェーンが用いるデータ構造

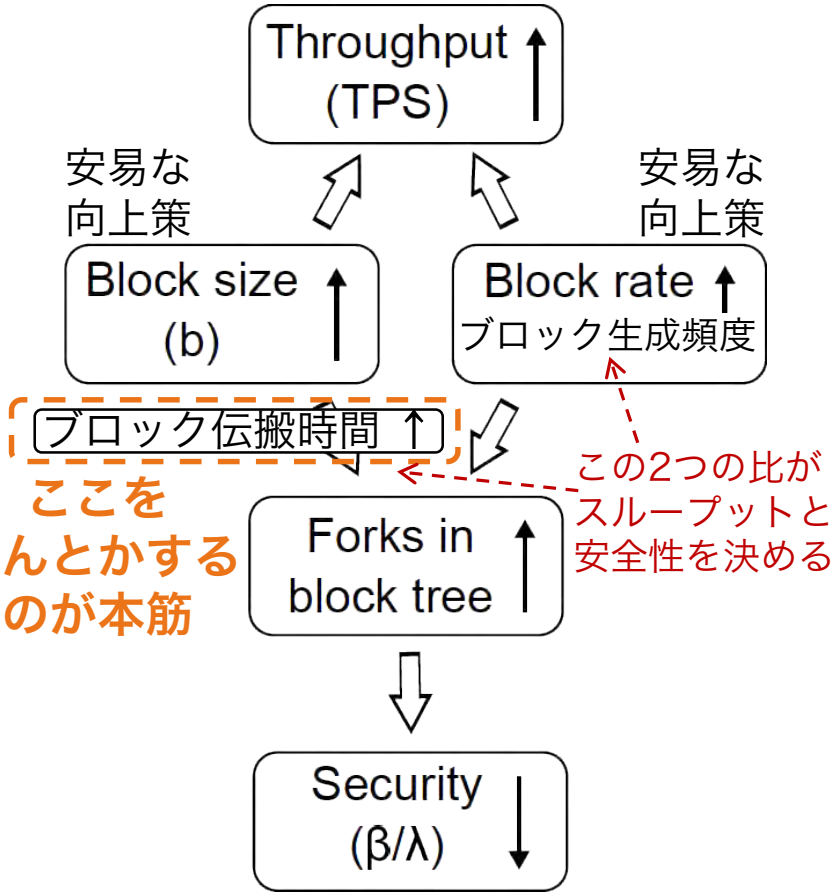
ノード間で、ブロックを伝搬させ、行き渡らせる

性能向上 vs. 安全性

- スループット(TPS)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 (右図)



フォークしたブロックチェーン

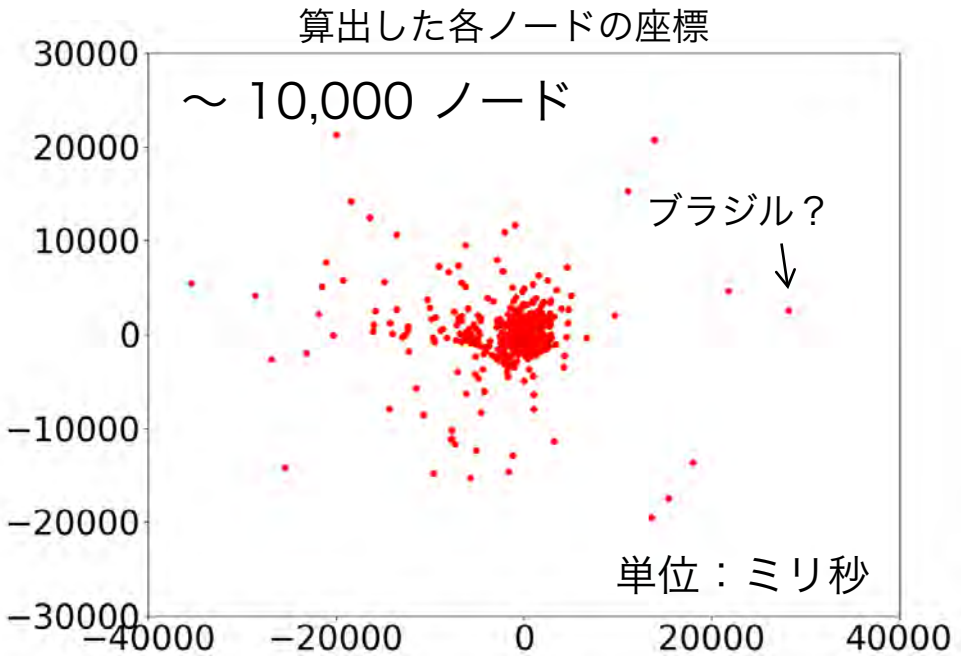


"Secure High-Rate Transaction Processing in Bitcoin", FC'15, 2015 の図

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



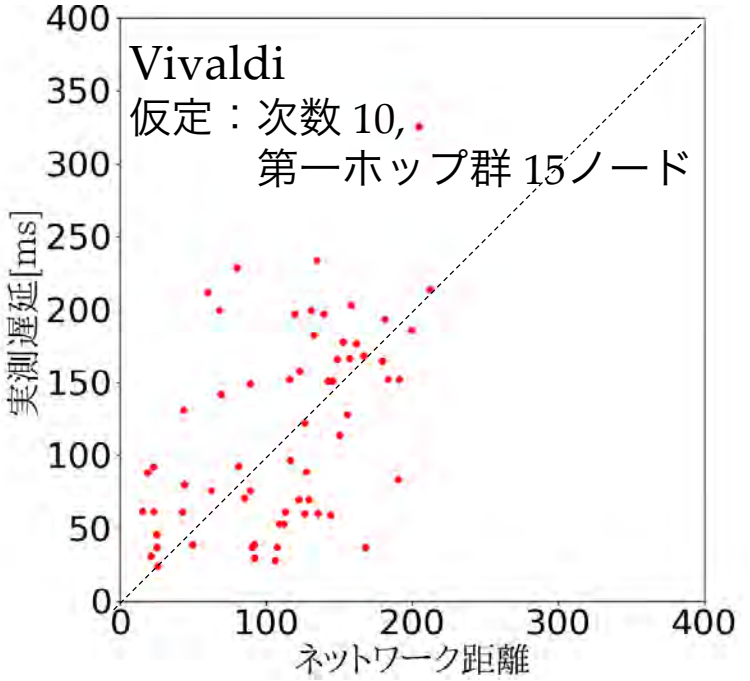
- 狙い
  - 伝搬高速化手法の指針
  - 隣接ノード選択の指針
- 現状と今後
  - 精度の向上
  - そのための
    トポロジ取得と推定

- ただ…

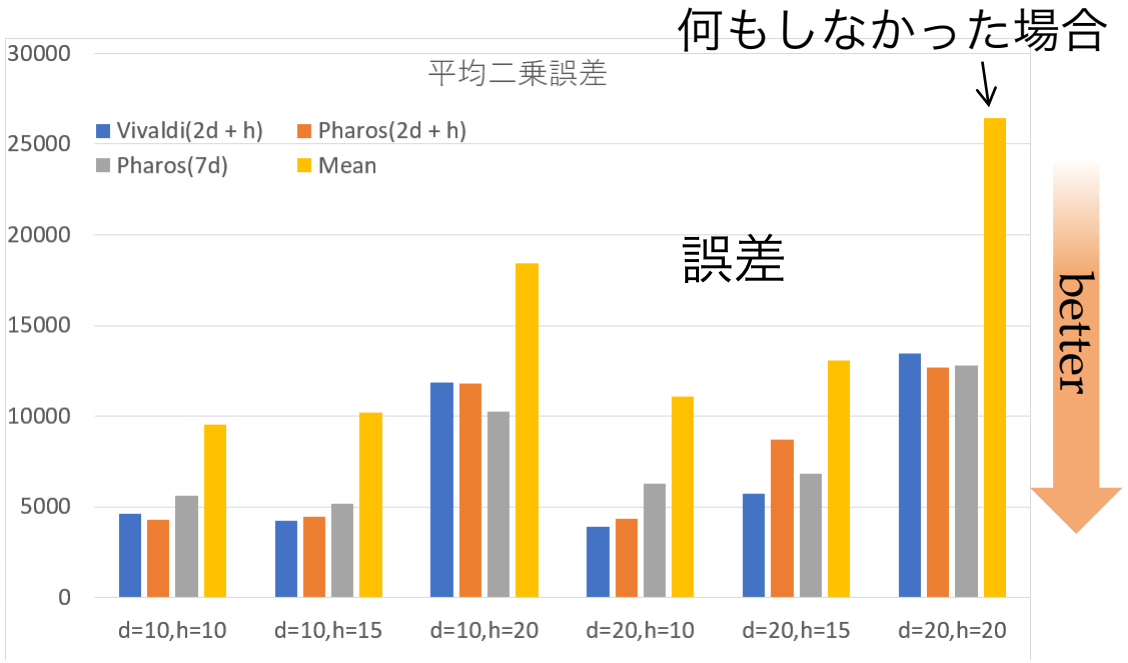
伝搬時間 推定 with ネットワーク座標系

[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

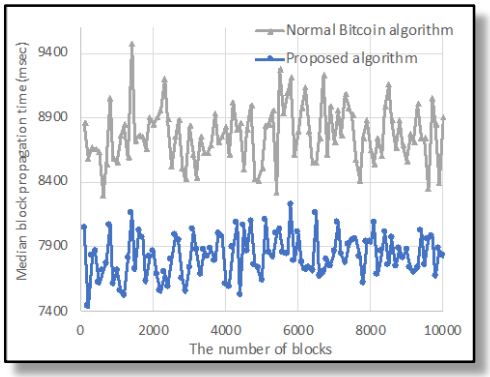
ツール の研究

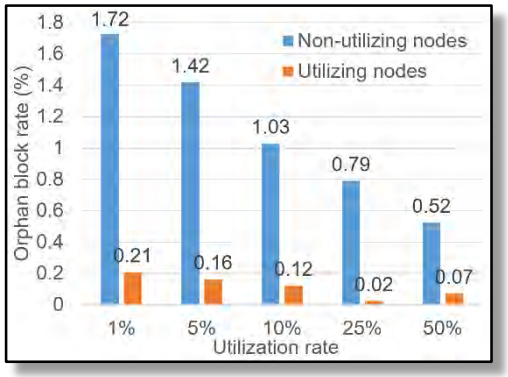
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

シミュレータ SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

- 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
  - ノード間でのブロック伝搬をシミュレート
    - インターネットの帯域幅・通信遅延：2015年, 2019年
      - 世界 6地域の、地域内 / 地域間 帯域幅と通信遅延
    - ブロックチェーンのノードの挙動：
      Proof of Work のマイニング所要時間, ブロックの転送, Compact Block Relay
      - Bitcoin, Litecoin, Dogecoin のパラメータ
  - 可視化ツール
  - 研究の例：

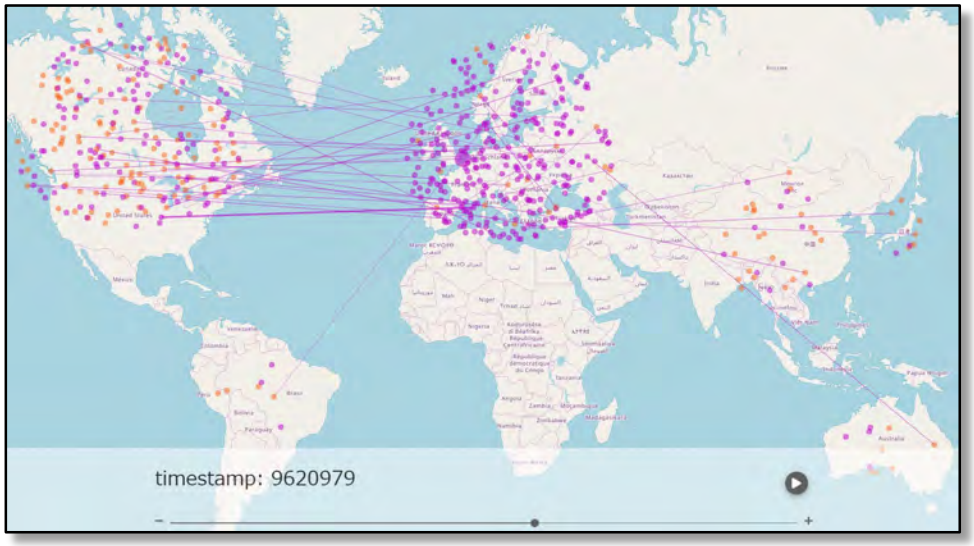




隣接ノード選択　リレーネットワーク 効果推定

シミュレータ SimBlock

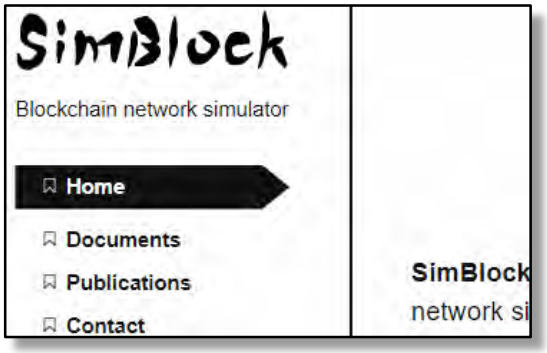
[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]

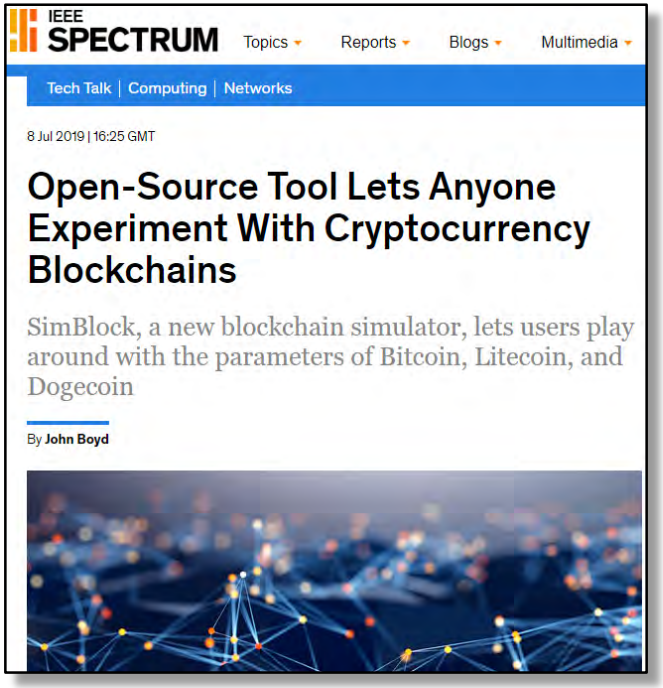


Visualizer

縮小 Bitcoin ネットワーク,
600 ノード

ウェブ
サイト





IEEE Spectrum
記事

IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

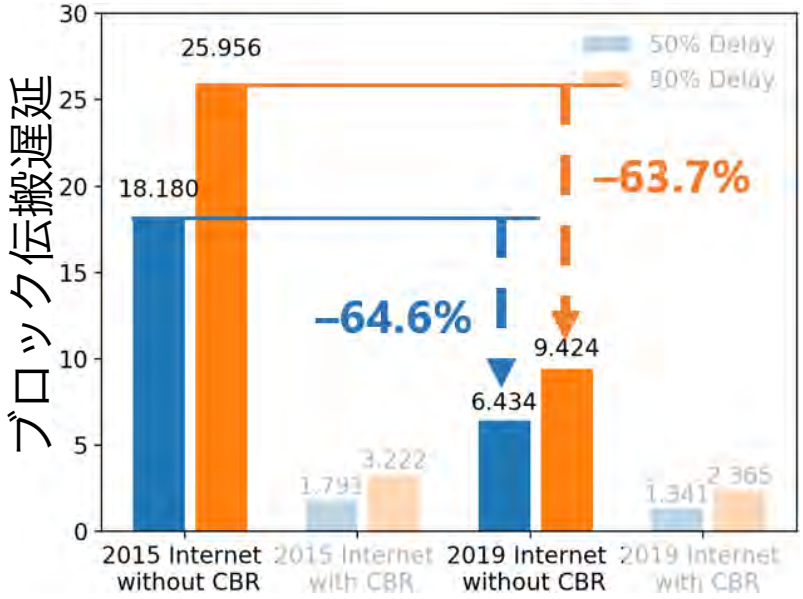
再び 性能 の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

インターネット高速化と Compact Block Relay の影響

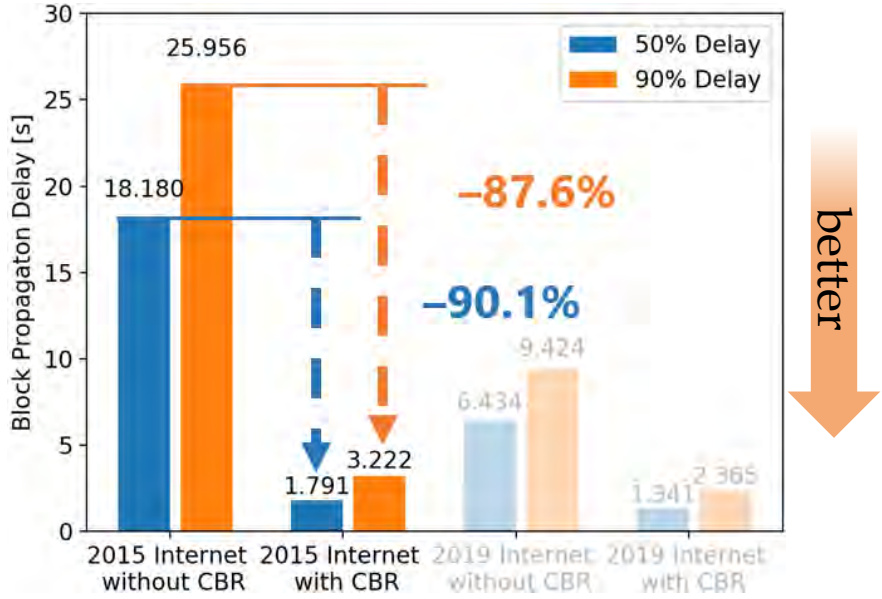
[永山 2020a]
[Nagayama 2020b]

- SimBlock を発展させたので、影響を調査
  - 2019年のインターネットの帯域幅・遅延
  - Bitcoin の Compact Block Relay プロトコル 2016年 8月の 0.13.0 が実装
    - ブロック伝搬の高効率化、ひいては高速化



インターネット高速化 (2015→2019) の影響

<

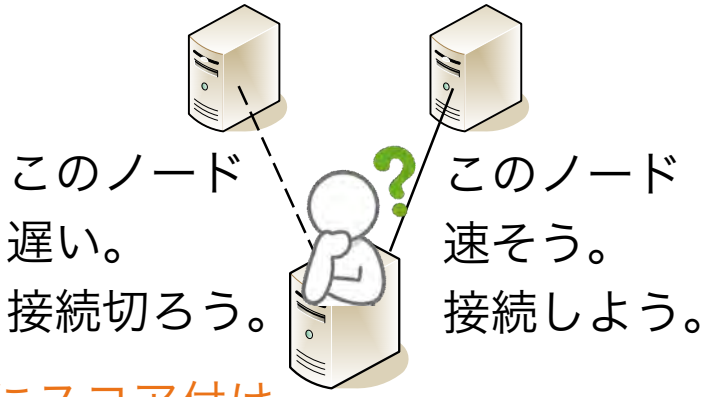


Compact Block Relay の影響

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
    - 僕らもやった：DHT での proximity neighbor selection [Miyao 2013]
- この研究のために、シミュレータ SimBlock を開発した

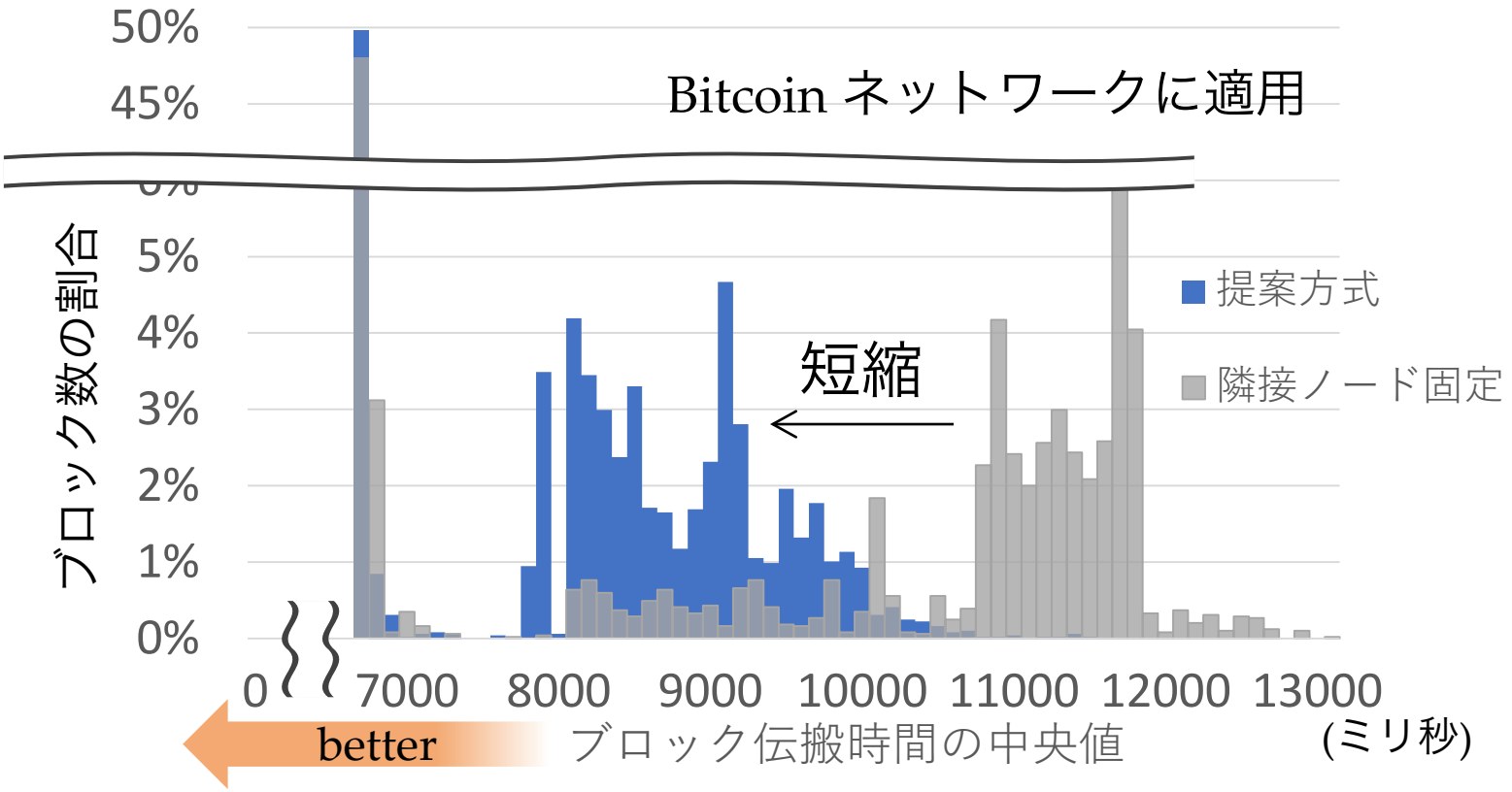


- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

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

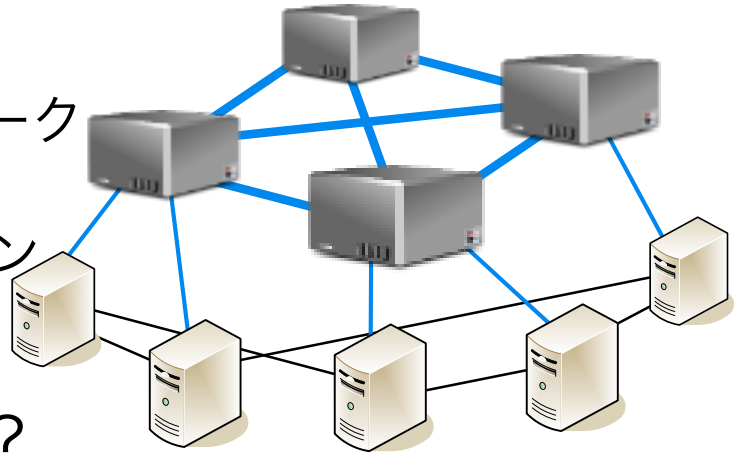


- 注：2015年のインターネットを対象として実験

リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- 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



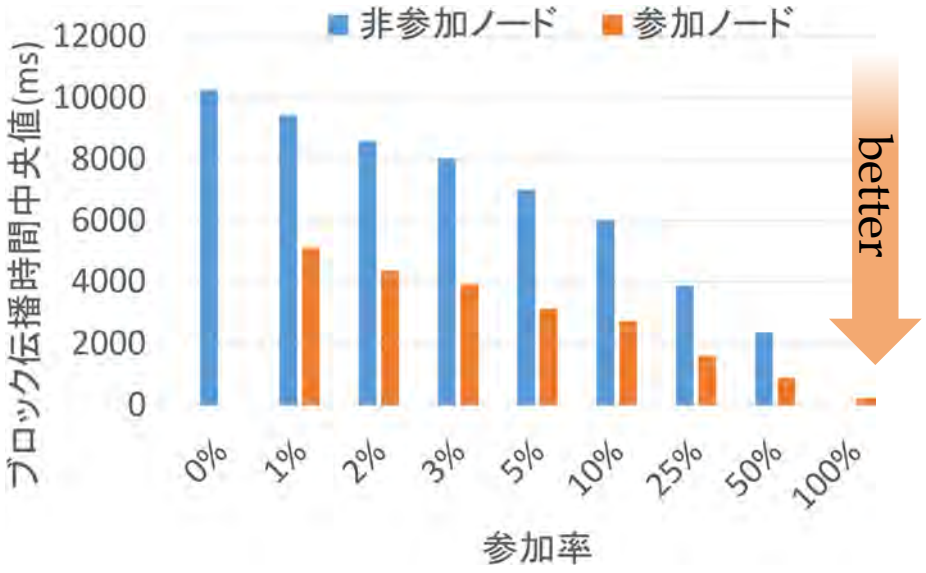
リレーネットワークの例: FALCON

- 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？

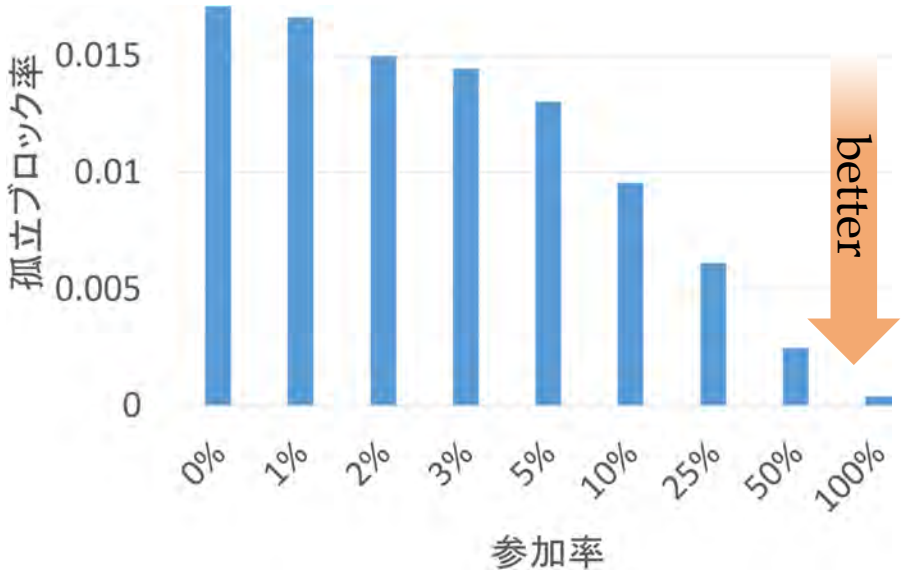
リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- 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！

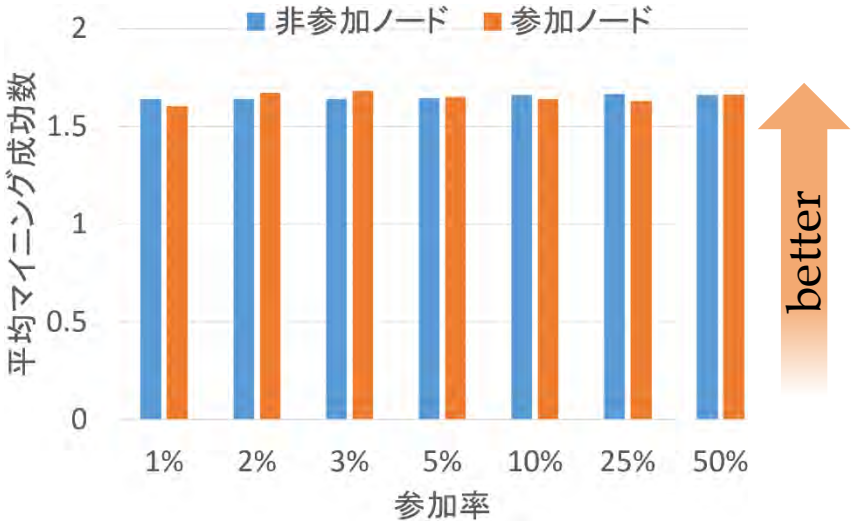
↑
フォークによって発生した、
メインチェーンから外れたブロック

- では、ノード レベルでは？

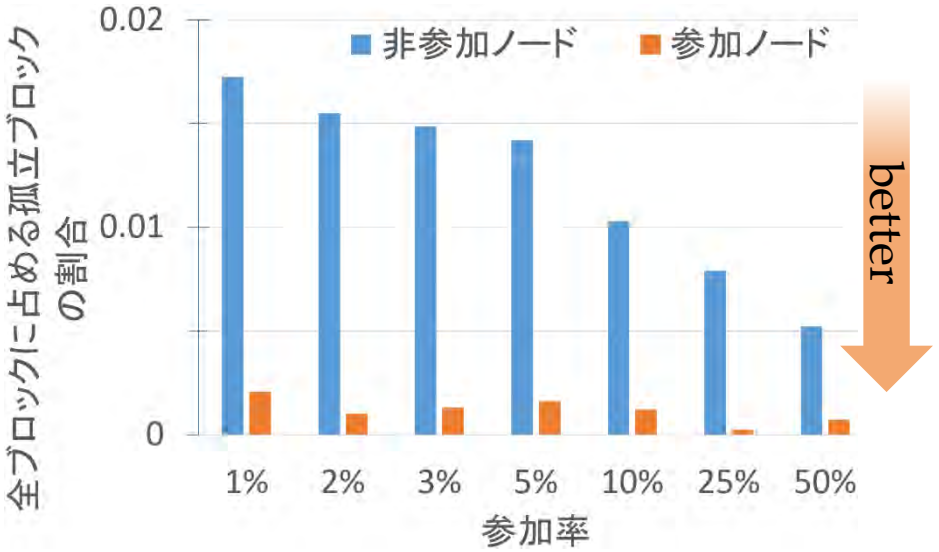
リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

- 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

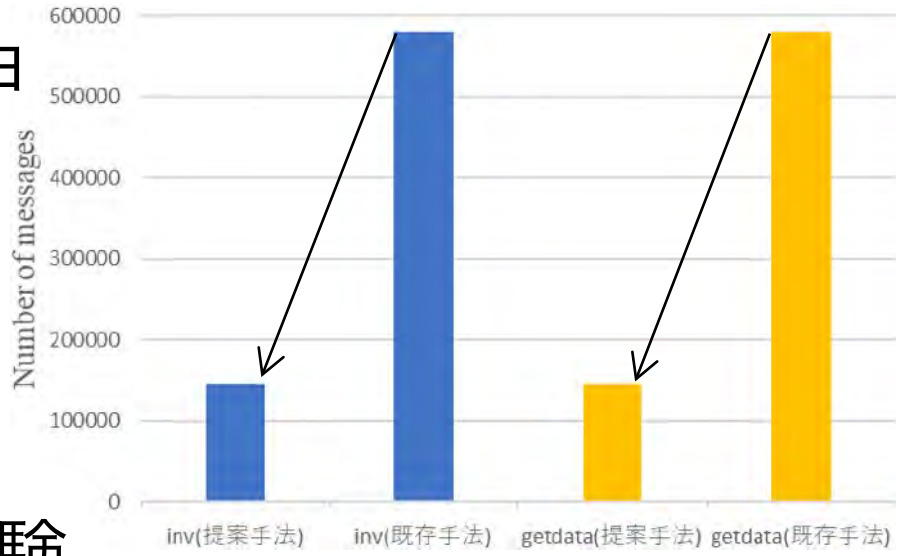
ブロードキャスト木の適用

in 工学院大学 坂野研　[北川 2021a] [北川 2021b]

- Plumtree (IEEE SRDS 2007)
  - 非構造化オーバレイ (P2P) ネットワーク上のブロードキャスト プロトコル
  - オーバレイ上にスパニングツリーを構築

- ブロック・トランザクションのブロードキャストに Plumtree を使用
  - e.g. Bitcoin はただのフラッディング

- SimBlock 上に実装して実験



メッセージ数 減少

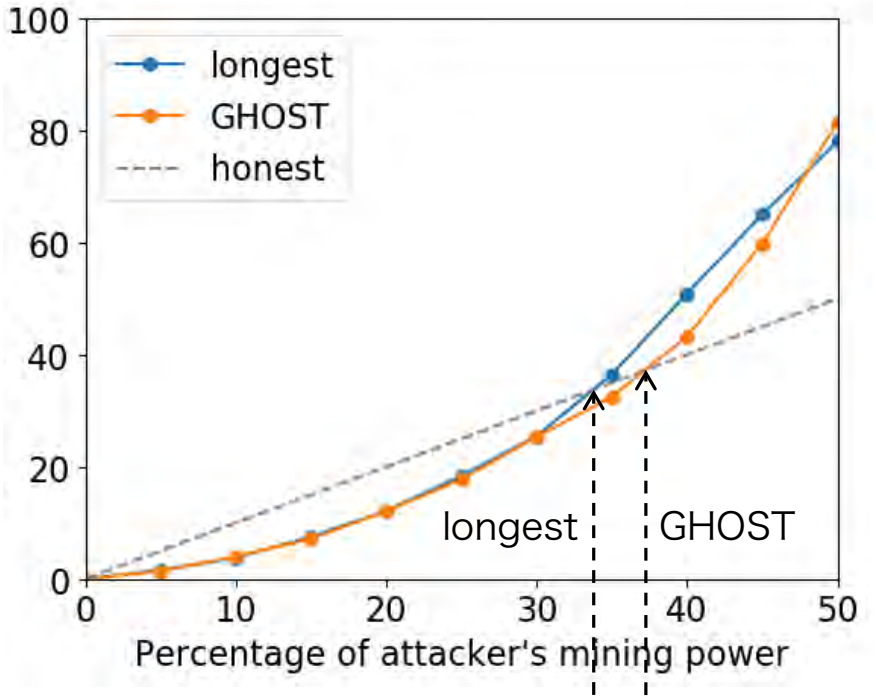
セキュリティ の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

selfish mining 攻撃を模擬

[Nagayama 2019]

- メインチェーンを決める規則 longest, GHOST の、攻撃への耐性を比較



攻撃で利得を得るために必要な
Proof of Work 計算能力 占有率

selfish mining 論文 (FC'13)
の値によく合致

シミュレート成功

Ethereum のシミュレート
という目論見への第一歩

→ 開発者会議 Devcon 5 で発表

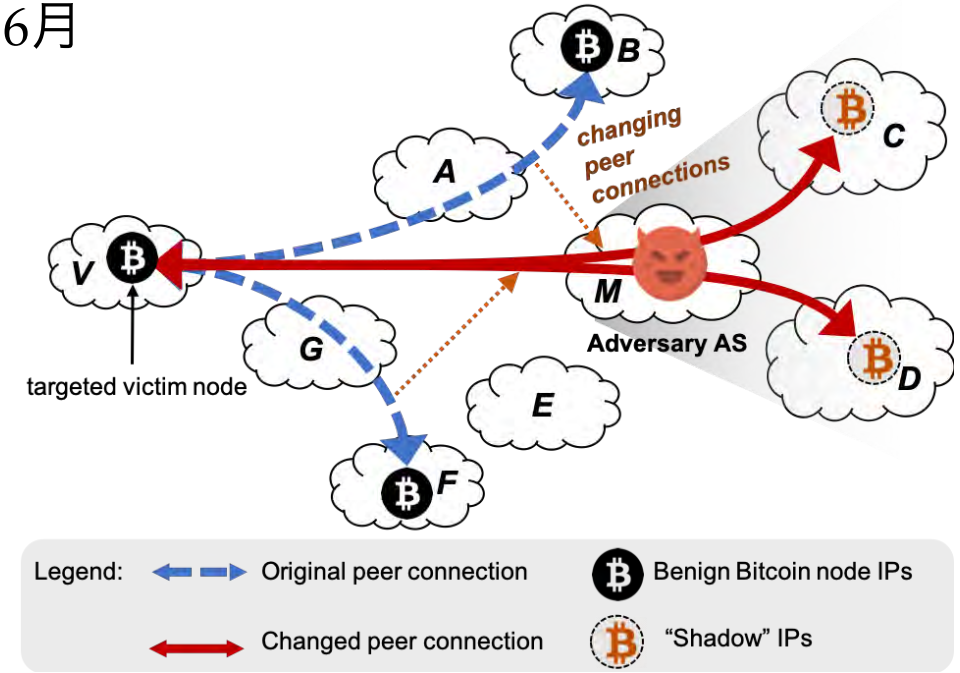
Devcon 5, 大阪,
2019年 10月

Erebus 攻撃対策の影響推定

[高山 2020b]

- Erebus 攻撃 (IEEE S&P 2020)
  - ネットワーク分割攻撃 → 様々な使いみち
  - AS を制御する攻撃者がノードを攻撃。
    対象ノードを攻撃者のノードに多く接続させる。
- 対策 in Bitcoin 0.20.0, 2020年 6月
  - ノードが学習する
    接続相手候補の数を
    AS ごとに制限。

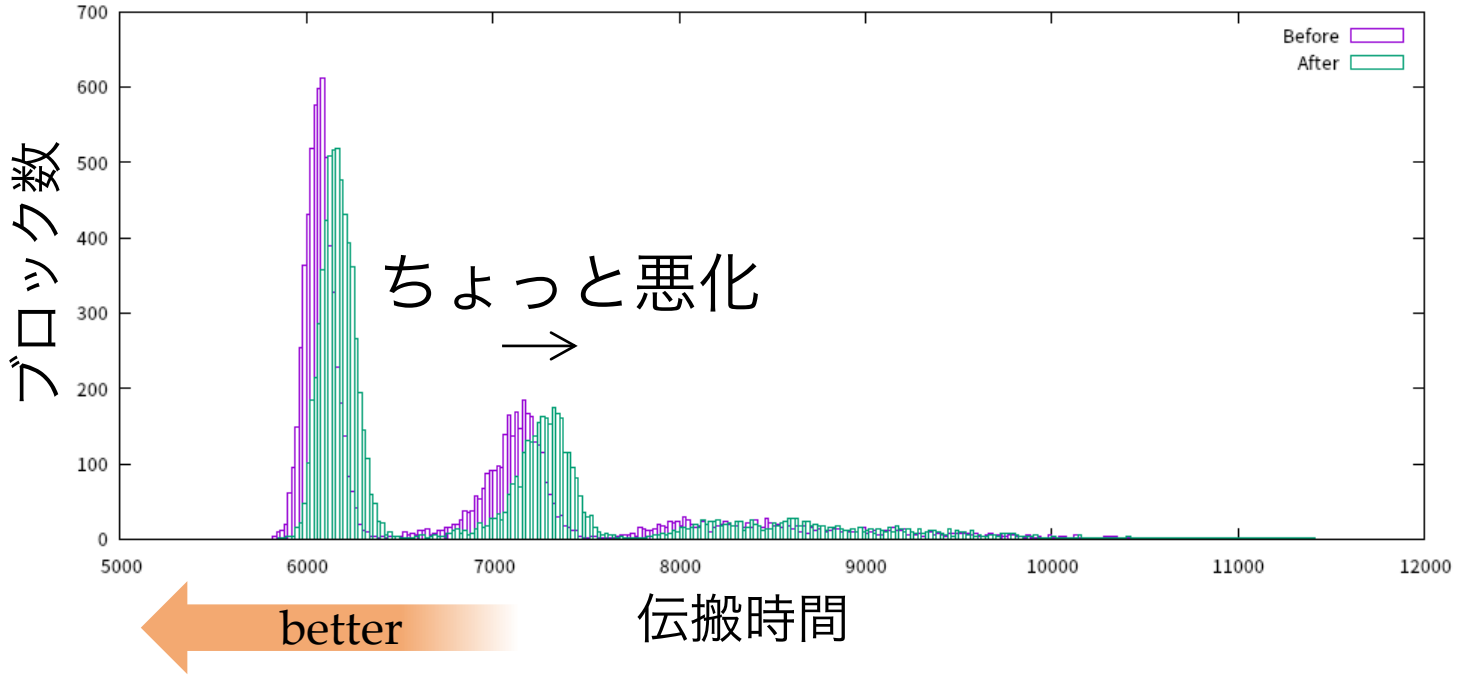
通信相手に、これまで
なかった制約が課せられ、
通信性能低下？



Erebus 攻撃対策の影響推定

[高山 2020b]

- ブロック伝搬時間、ちょっと悪化
  - 50%ile：3556 → 3562 ms (+ 6 ms)
  - 90%ile：6729 → 6846 ms (+ 117 ms)

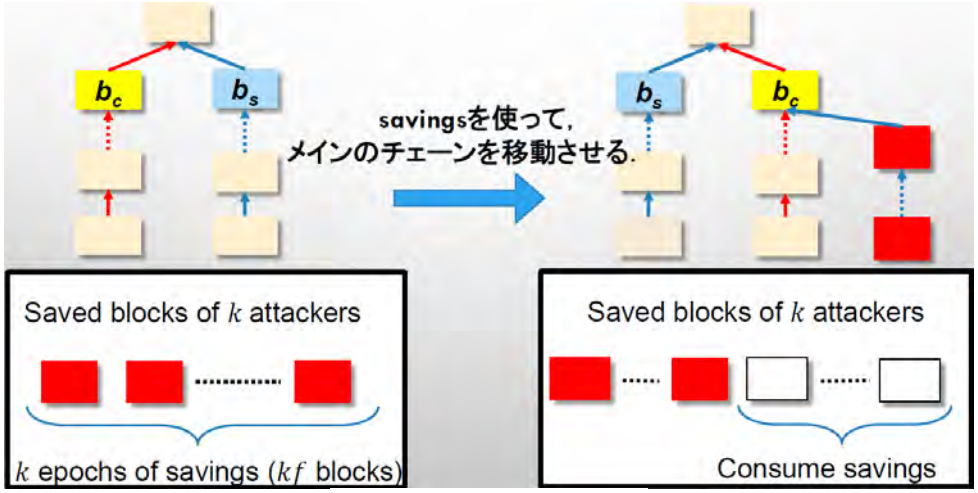


- routing 攻撃をシミュレートできた

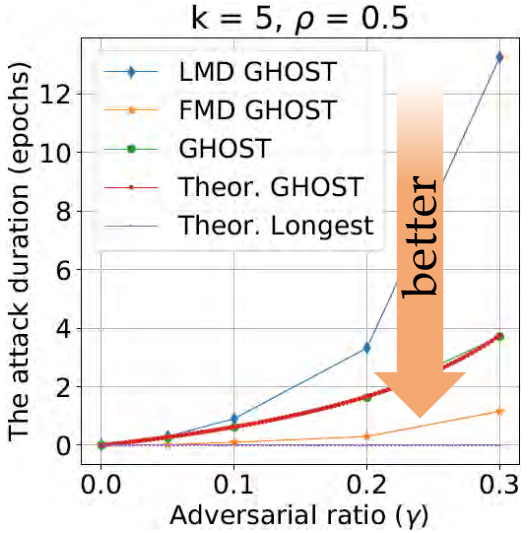
Ethereum 2.0 等 PoS ブロックチェーンへの攻撃手法と耐性調査

[大月 2021a]

- saving attack を発見
  - ブロックを作る権利を保存 (save) しておく
  - 都合よいタイミングでブロック生成
  - 複数チェーンの競合状態を、より長く維持
- メインチェーンを決める規則ごとの、攻撃への耐性を調査
  - 狙った通り、FMD GHOST がベスト



saving attack



LMD GHOST

GHOST

FMD GHOST

公平性 の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

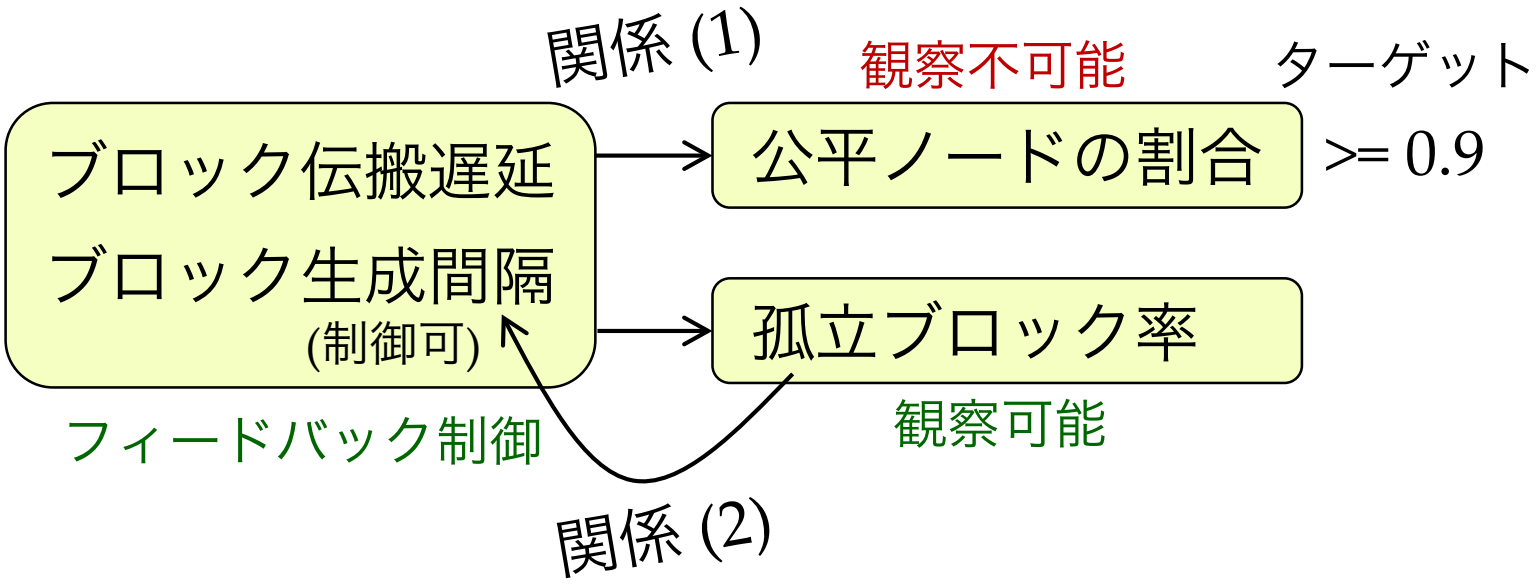
- 公平とは
  - マイニング成功率がハッシュレート (計算能力) に比例
  - …しかし、伝搬遅延によりブロックの受信が遅れると、その分、マイニングに費やせる時間が減る → 不公平
    - Ethereum なら、ブロック間隔 13秒前後 – 伝搬遅延が実質マイニング時間

- 既存の公平性 [Cromon 2016] ← 雑すぎる
  - 90% のノードが一瞬でもマイニングできれば公平
- 提案：**(X, ε) 公平性**
  - 充分長いブロックチェーンに対して、割合 X のノードが不公平を被る確率 ε 以下。
  - 今回、$X = 0.9$, $\varepsilon = 0.01$ 。

ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

- (0.9, 0.01) 公平性を保つブロック生成間隔調整法
  - 公平ノードの割合は事後にしか算出できない。
  - 代わりに、ブロック生成間隔を通じて**孤立ブロック率を制御**する。



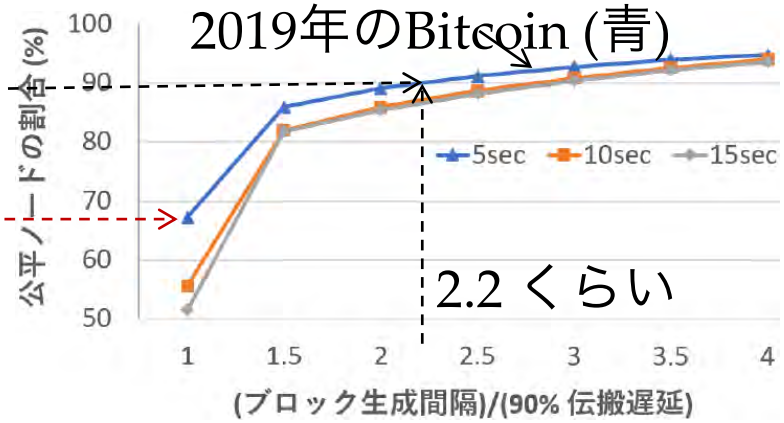
ノード間の公平性指標とブロック生成間隔調整

[神田 2020a]
[Kanda 2020b]

- 関係 (1)
  - ブロック伝搬遅延の分布はガンマ分布であると仮定し、Bitcoin での実測値を元に、公平ノードの割合を算出

狙い：
X = 0.9

既存の公平性



ブロック生成間隔 / 90%ile 伝搬遅延 が
2〜3 以上ならよさそう

- 関係 (2)
  - 孤立ブロック率は、ブロックの伝搬遅延と生成間隔の関数 [Decker 2013]

	$\frac{\text{ブロック生成間隔}}{\text{90\%伝搬遅延}} = 2$	$\frac{\text{ブロック生成間隔}}{\text{90\%伝搬遅延}} = 3$
5sec	14.6%	9.8%
10sec	14.2%	9.6%
15sec	14.1%	7.2%

孤立ブロック率
14.6% 〜 9.8% 以下を狙う

シミュレータ SimBlock 上で
制御の実験 → 成功

例：ネットワーク帯域幅が変化しても公平ノードの割合が高く保たれた

分権化 の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

Proof of Stake 各プロトコルの中央集権の度合い

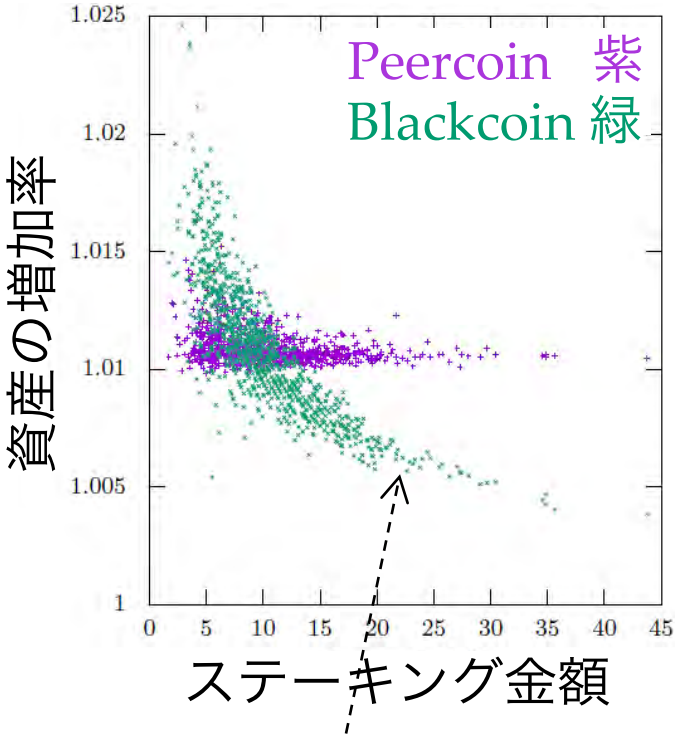
[高山 2020a]

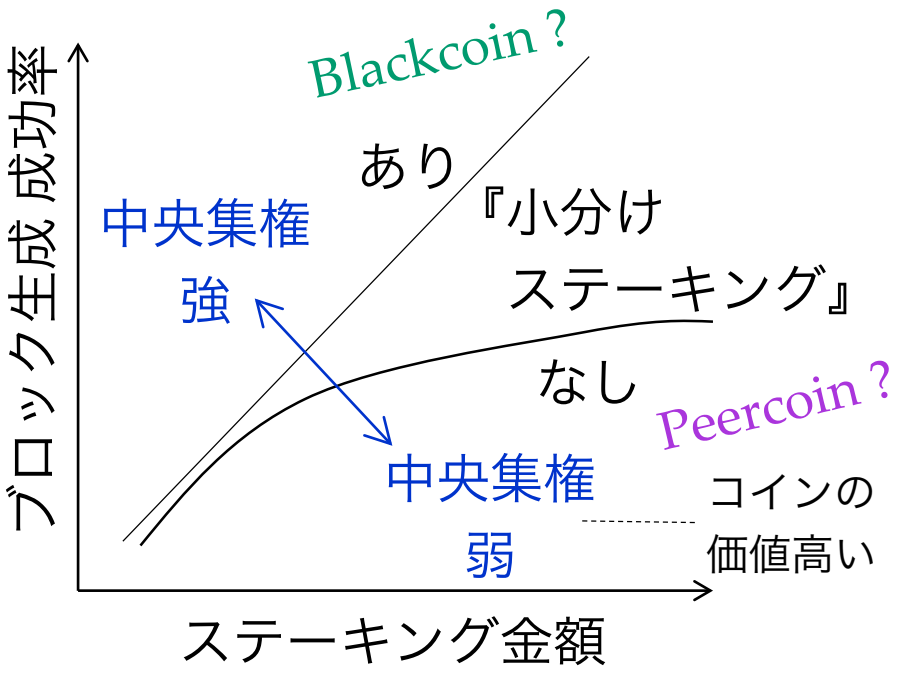
- Proof of Stake (PoS)
  - 各ノードは、持ち金 or deposit 金額に応じて、ブロック生成権を得られる
- プロトコルによって、
  中央集権の度合いがどう変わってくるか？
  - Peercoin [King 2012] – PoS を提案
    - 当選確率：コイン年齢 / coin age (= 金額 × **未使用期間**) に比例
      - 51% 攻撃を防ぐ、という主張：
        攻撃用にコインを買っても、コイン年齢が若くて役立たない。
    - 報酬：コイン年齢に比例
  - Blackcoin (2014年 〜) 1.2
    - 当選確率：単に金額に比例, ただし最低未使用期間はあり
      - コイン年齢の危険性を指摘：
        皆、オフラインのままコイン年齢を稼ぐ → 51% 攻撃の危険。
    - 報酬：固定額

Proof of Stake 各プロトコルの中央集権の度合い

[高山 2020a]

- 結論：Blackcoin 1.2 > Peercoin
  - 『小分けス(略)』Peercoin はなし、Blackcoin 1.2 はあり、に落ち着くだろう。

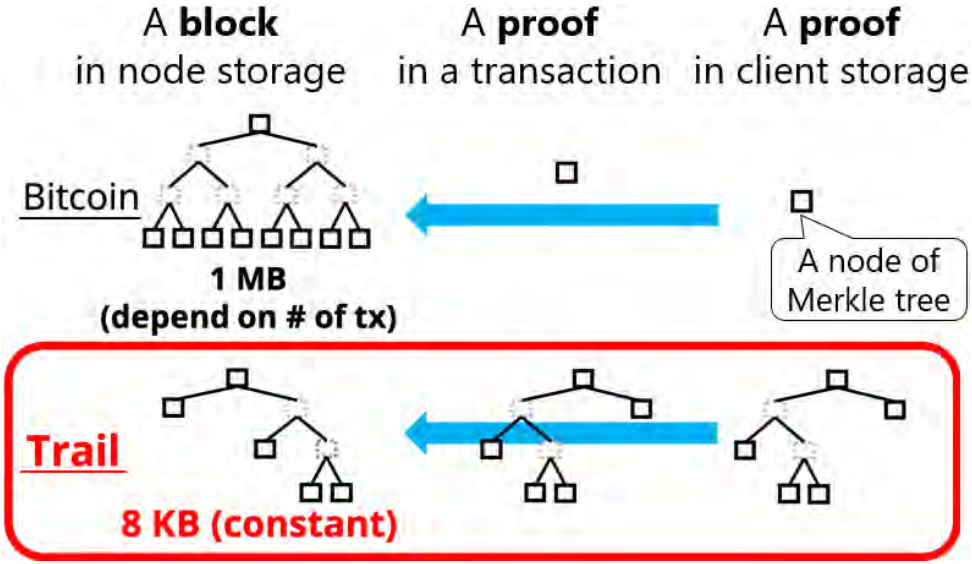




ステーキング金額が大きいと損。おかしい。
→『小分けステーキング』で改善できる

ノードの保持データ量が少ないブロックチェーン用データ構造

- 大きな台帳データがノード運営の負担で、分権化 / decentralization を妨げている。 [Nagayama 2020a]
  - Bitcoin 320 GB, Ethereum 188 GB (2020年 12月)
- 提案：
  - ノードの保持データ量が少ないデータ構造 Trail
  - 代わりに、クライアントが自己責任で TX を保存・バックアップ



まとめ

- 性能、ツール、セキュリティ、公平性、分権化、…の研究を紹介
- ネットワーク面からの性能の研究は、そろそろ…

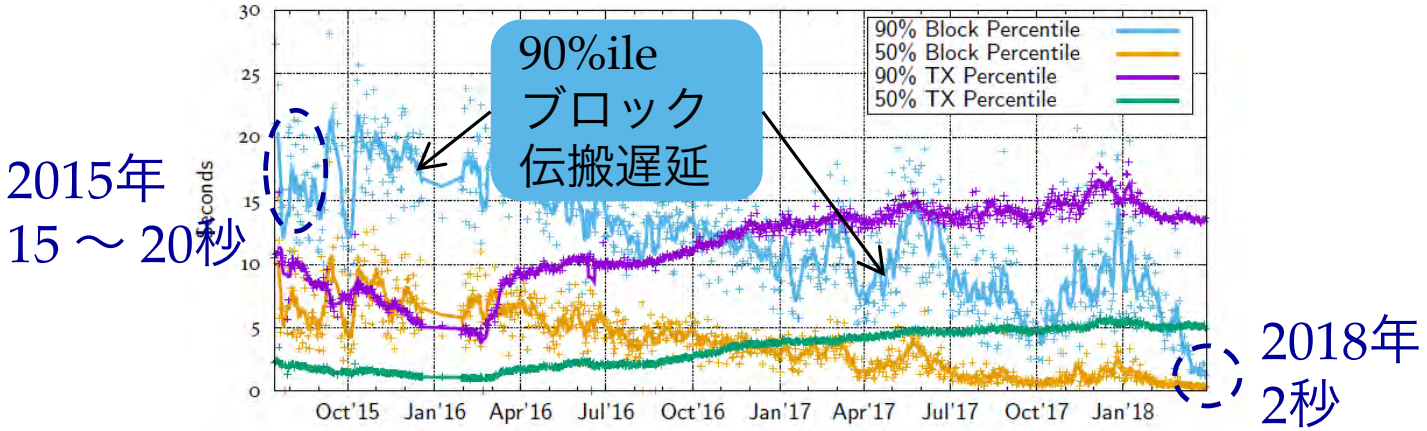


Figure 4.12: Bitcoin propagation delay for block and transaction propagation (50 % and 90 % percentiles).

T. Neudecker: “Security and …”, Ph.D. thesis, 2018年

- 現在 ～ 今後：

  セキュリティ (攻撃手法と対策の考案と評価), Ethereum 2.0, ソフトのアーキテクチャ, 応用, …

発表 (1)

- ツール
  - [青木 2019a] 青木優介, 大月魁, 金子孟司, 坂野遼平, 首藤一幸: “**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, p.219-224, 2019年 3月
  - [Aoki 2019b] Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, Kazuyuki Shudo: "**SimBlock: A Blockchain Network Simulator**", Proc. CryBlock 2019 (in conj. with INFOCOM 2019), 2019年 4月
  - [Banno 2019] Ryohei Banno, Kazuyuki Shudo: “**Simulating a Blockchain Network with SimBlock**”, Demonstration, Proc. IEEE ICBC 2019, pp.3-4, 2019年 5月
  - [Shudo 2019] Kazuyuki Shudo: "**SimBlock**", lightning talks, P2P Summit, Devcon 5, Ethereum Foundation, 2019年 10月

発表 (2)

- 性能
  - [神田 2019a] 神田伶樹, 首藤一幸: “**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] Reiki Kanda, Kazuyuki Shudo: “**Estimation of Data Propagation Time on the Bitcoin Network**”, Proc. AINTEC 2019, pp.47-52, 2019年 8月
  - [青木 2019c] 青木優介, 首藤一幸: “**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] Yusuke Aoki, Kazuyuki Shudo: “**Proximity Neighbor Selection in Blockchain Networks**”, Proc. IEEE Blockchain 2019, pp.52-58, 2019年 7月
  - [大月 2020a] 大月魁, 首藤一幸, 坂野遼平: “**ビットコインに対するリレーネットワークの影響**”, 信学技報, Vol.119, No.460, NS2019-192, pp.89-94, 2020年 3月
  - [Otsuki 2020b] Kai Otsuki, Ryohei Banno, Kazuyuki Shudo: “**Quantitatively Analyzing Relay Networks in Bitcoin**”, Proc. IEEE Blockchain 2020, pp.214-220, 2020年 11月
  - [永山 2020a] 永山流之介, 首藤一幸, 坂野遼平: “**コンパクトブロックリレーとインターネット高速化を考慮したビットコインネットワークシミュレーション**”, 信学技報, Vol.119, No.460, NS2019-208, pp.179-183, 2020年 3月
  - [Nagayama 2020b] Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo: "**Identifying Impacts of Protocol and Internet Development on the Bitcoin Network**", Proc IEEE ISCC 2020, pp.506-510, 2020年 7月

発表 (3)

- 性能 (続き)
  - [Banno 2020] Ryohei Banno, Yusuke Kitagawa, Kazuyuki Shudo: "**A Study of Blockchain Systems Exploiting Semi-Structured Overlay Networks with FRT**", Proc. 2020 Int'l Conf. on Emerging Technologies for Communications (ICETC 2020), 2020年 12月
  - [Banno 2021] Ryohei Banno, Yusuke Kitagawa, Kazuyuki Shudo: "**Exploiting semi-structured overlay networks in blockchain systems**", IEICE Communications Express, Vol.X10-B, No.8, 2021年 8月 (published online on February 9, 2021)
  - [北川 2021a] 北川雄介, 首藤一幸, 水野修, 坂野遼平: "ブロックチェーンネットワークに対する **Plumtree**アルゴリズムの適用に関する一検討", 2021年 電子情報通信学会 総合大会, BS-9-9, 2021年 3月
  - [北川 2021b]北川雄介, 首藤一幸, 水野修, 坂野遼平: "**ブロックチェーンネットワークにおける Plumtreeアルゴリズムの適用検証**", 電子情報通信学会 技術研究報告, Vol.121, No.68, IA2021-7, pp.39-42, 2021年 6月

発表 (4)

- セキュリティ
  - [Nagayama 2019] Ryunosuke Nagayama, Kazuyuki Shudo: "**Simulating Ethereum Network with SimBlock**", lightning talks, Devcon 5, Ethereum Foundation, 2019年 10月
  - [高山 2020b] 高山柊: “**Erebus攻撃への対策がBitcoinネットワーク性能に与える影響**”, 首藤研 演習成果発表会, 2020年 7月
  - [大月 2021a] 大月魁, 中村龍矢, 首藤一幸: “**Saving attack のブロックチェーンコンセンサスに対する影響**”, 信学技報, Vol.120, No.381, IA2020-37, pp.15-22, 2021年 3月

発表 (5)

- 公平性
  - [神田 2020a] 神田伶樹, 首藤一幸: "**公平なProof-of-Workブロックチェーンに向けたブロック生成間隔調整**", 信学技報, Vol.119, No.460, NS2019-206, pp.169-174, 2020年 3月
  - [Kanda 2020b] Reiki Kanda, Kazuyuki Shudo: "**Block Interval Adjustment Toward Fair Proof-of-Work Blockchains**", Proc. ICDE 2020 Workshops (BlockDM 2020), pp.1-6, 2020年 4月
- 分権化
  - [Nagayama 2020a] Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo: "**Trail: A Blockchain Architecture for Light Nodes**", Proc. IEEE ISCC 2020, pp.511-517, 2020年 7月
  - [高山 2020a] 高山柊, 永山流之介, 大月魁, 首藤一幸: "**Proof-of-Stakeブロックチェーンの中央集権化へのコイン年齢の影響**", 信学技報, Vol.119, No.460, NS2019-207, pp.175-178, 2020年 3月
- 応用
  - [高山 2021] 高山柊, 竹井悠人, 首藤一幸: "**パブリックブロックチェーンを用いたプログラマブルな正答集合を扱える試験プロトコル**", 第23回プログラミングおよびプログラミング言語ワークショップ (PPL 2021), 2021年 3月