

…勉強会

2023年 6月 22日(木)

0 / 48

# ブロックチェーン「ネットワーク」 の研究

首藤 一幸

京都大学 / 東京工業大学

**SimBlock** [bit.ly/  
study-202306-shudo](https://bit.ly/study-202306-shudo)   Kyoto U. Tokyo Tech

# 首藤 一幸 (49)

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

2022/ 4 京大 

2009/ 5 未踏 PM 

2023/ 4 未踏アドバンス PM

2018/11 (株)アーリーワークス 顧問

2019/ 1 Miraise (シード特化ファンド) メンター

2022/ 7 GMOインターネットグループ(株) 技術顧問

2022/10 GMO AI & Web3(株) 顧問

2023/ 6 (一社)情報処理学会 理事

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

P2P のアルゴリズム, 2009 ~

構造化オーバーレイ / 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 2023年 6月

魔法のようなソフト

大規模分散システム

# 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 → トラストレス

- 首藤研での研究

- 性能
  - ツール
  - セキュリティ
  - 公平性
  - 分権化
  - 外部依存の削減
- } → トラストレスに貢献

- 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

cryptocurrency

# または仮想通貨, 暗号資産

crypto asset

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

1万 9千種類あるとか



# 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？

- 2009年 1月のメール

Satoshi Nakamoto  
が誰なのかは、  
今日に至るまで不明

## 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.

## Bitcoin v0.1 released

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Thu Jan 8 14:27:40 EST 2009

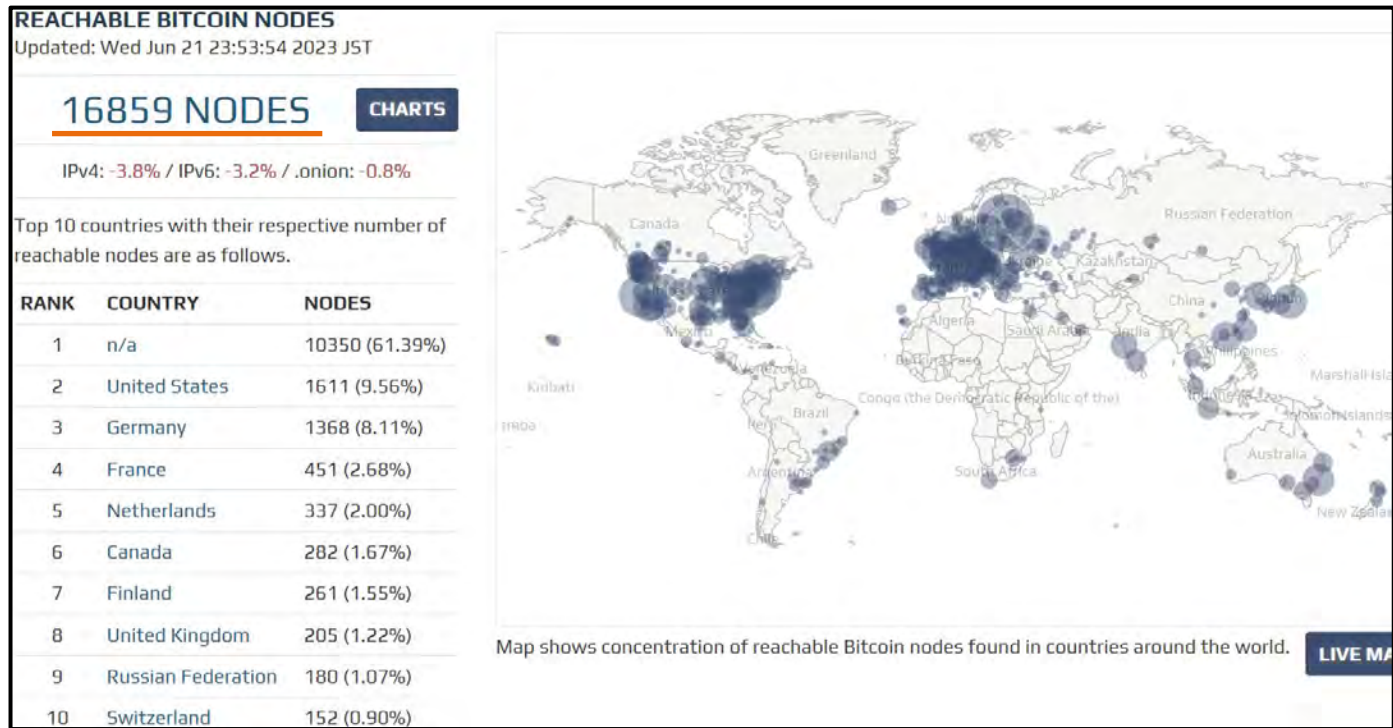
Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See [bitcoin.org](http://bitcoin.org) for screenshots.

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

# Bitcoin の非集中 分散システム

- インターネット上に **1万数千** 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

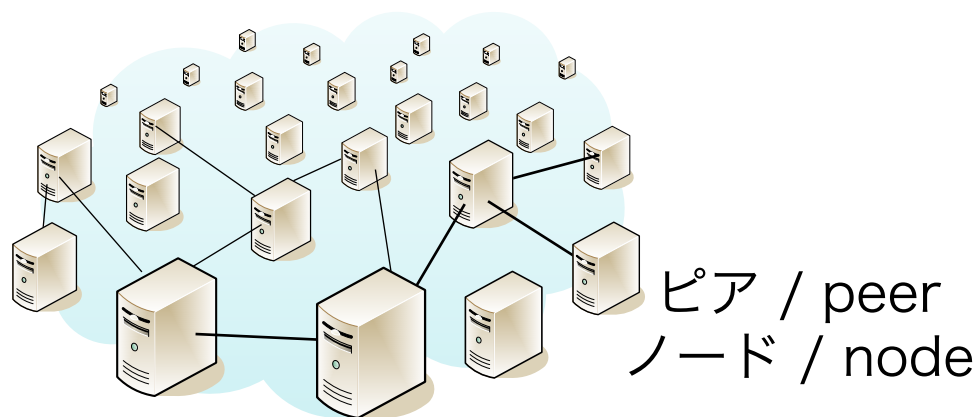


<https://bitnodes.io/> より

- **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



非集中 分散システム (peer-to-peer)



- 誰かを信用する必要がない → 「<sup>トラストレス</sup>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  **トラストレス**  
decentralized trustless

 **耐故障性**  
非集中に加えて  
fault tolerant

・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

 **トレーサビリティ**  
traceability

← ● **整合性** を保つ  **整合性確認のために (全) 履歴を残すので**  
consistent

← ● **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
  - 外部依存の削減
- トラストレスに貢献

# 研究成果

- 「ツール」「性能」から「セキュリティ」「トラストレス」へ

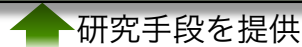
## セキュリティ

selfish mining 攻撃への耐性評価 [Nagayama 2019]  
 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 [Otsuki 2021c]他  
 理論フォーク率の正確な表現 [Sakurai 2023a]他



## 性能

伝搬時間 推定 [Kanda 2019b]他  
 隣接ノード選択 [Aoki 2019d]他  
 プロトコルの効果推定 [Nagayama 2020b]他  
 リレーネットワークの影響推定 [Otsuki 2020c]他  
 ブロードキャスト木の適用 [Kitagawa 2023]他  
 ブロック送信元 切り替え [Sakurai 2023a]他  
 ブロック生成通知 [Hasegawa 2023]他  
 ブロック生成間隔 調整 [Arakawa 2022b]他



## ツール

シミュレータ **SimBlock** [Aoki 2019c] [Banno 2019]  
 [Shudo 2019] [Shudo 2023]

研究手段を提供

## インセンティブ不整合問題

[Shudo 2018b]他  
 ブロックチェーン間アプリ移行

## トラストレス / trustless

中央集権の度合い評価 [高山 2020a]  
 新データ構造 [Nagayama 2022]他  
 データ集約 [Song 2022b]他  
 時計合わせ [Miki 2022b]他  
 公平性指標と向上手法 [Kanda 2020c]他



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

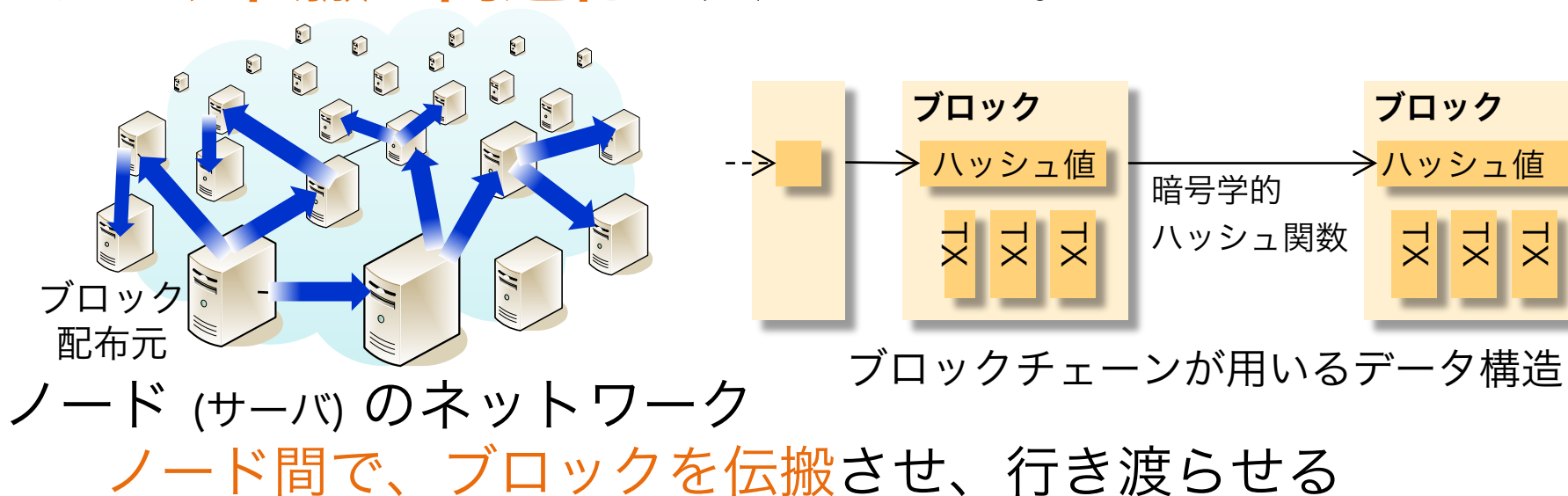


# 性能の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

# ブロックチェーンの性能

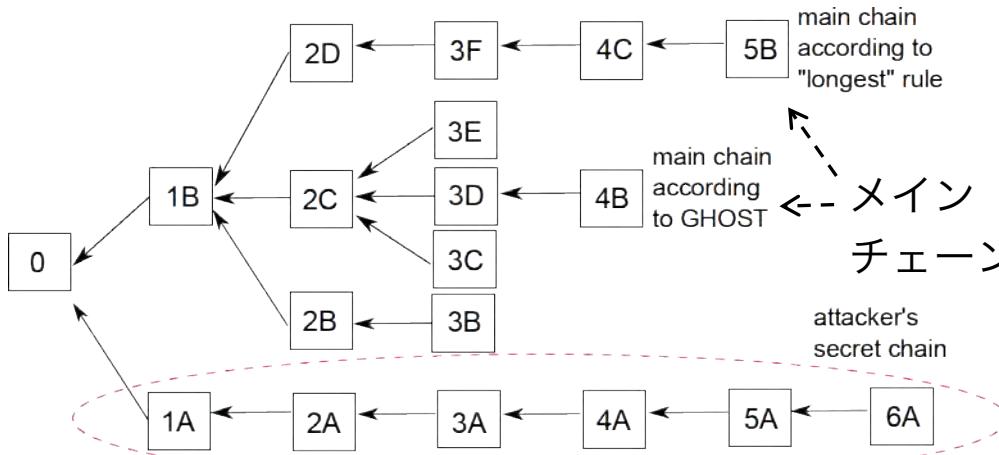
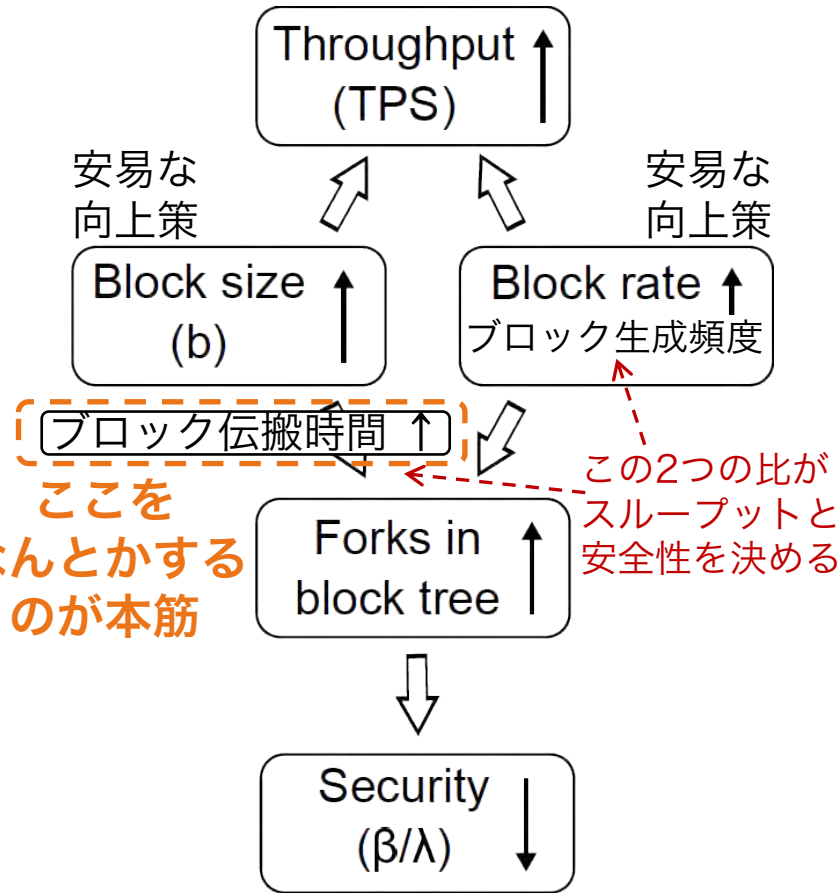
- 性能：トランザクション (取引, TX) / 秒 = TPS
  - TX の例：AさんからBさんに1BTC送金
  - 既存 VISA (クレジットカード) 1,700 TPS, PayPal 平均 320 TPS
  - 暗号通貨 Bitcoin 7 → 27 TPS, Ethereum 15 TPS 前後 **圧倒的に不足**
- 性能向上には、ノード (サーバ) 間での  
**データ伝搬の高速化**が欠かせない。 理屈は次ページ



# 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

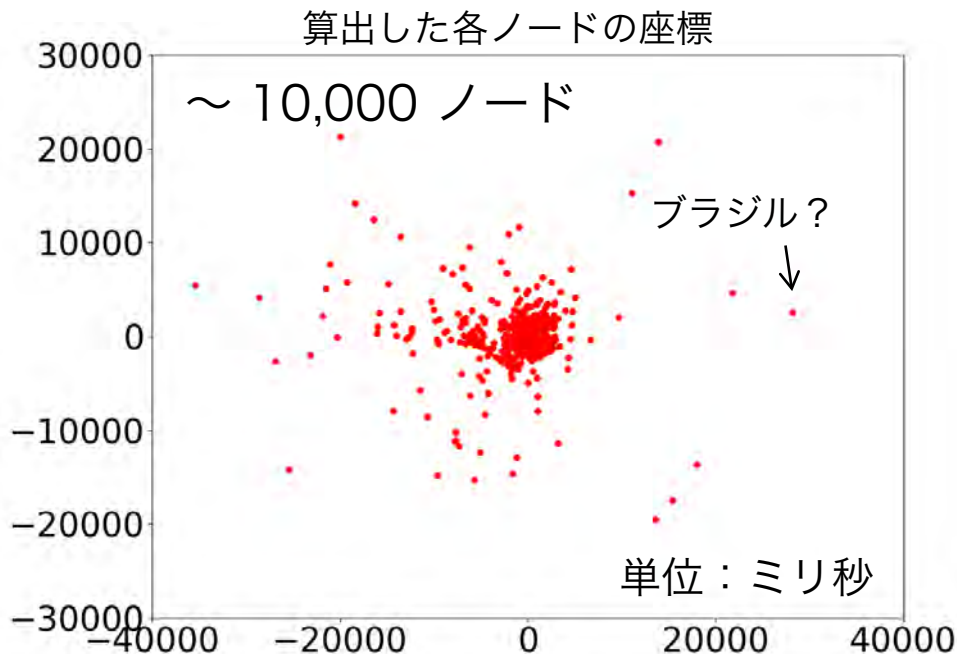
# 伝搬時間 推定 with ネットワーク座標系

15 / 48

[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

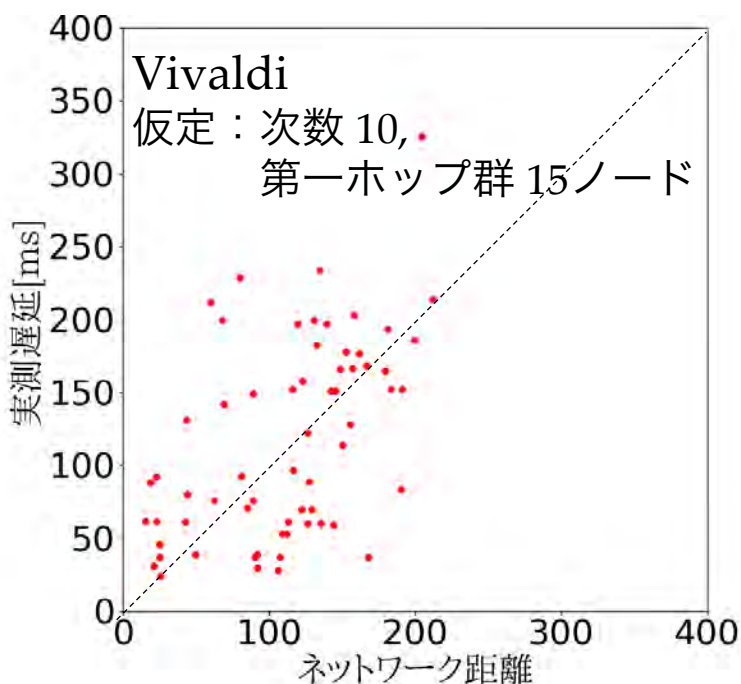
- ただ...



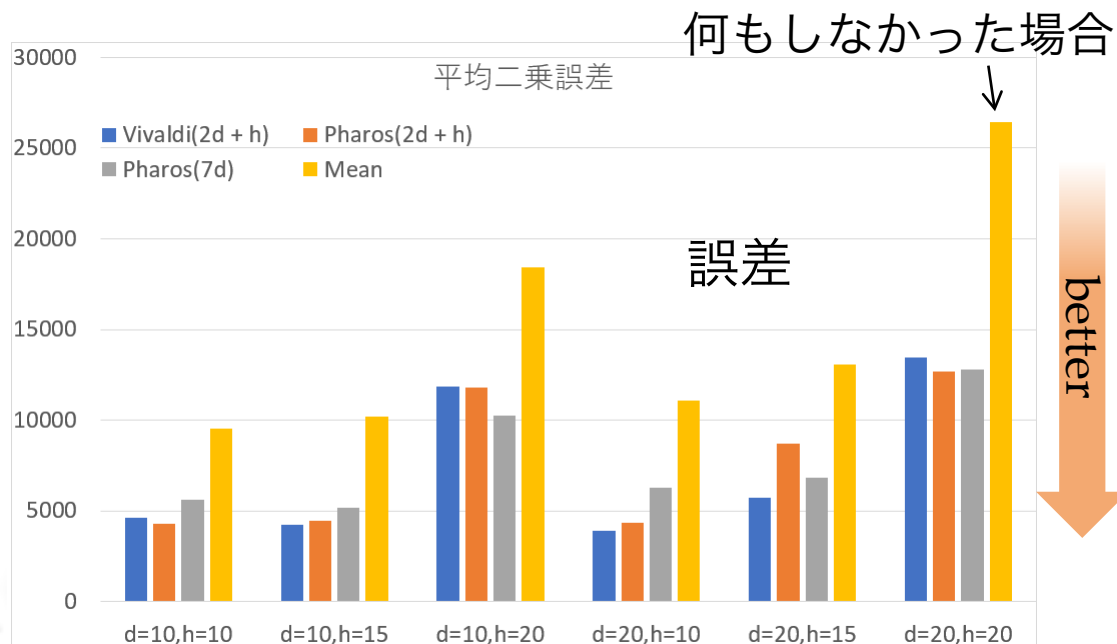
# 伝搬時間 推定 with ネットワーク座標系

[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

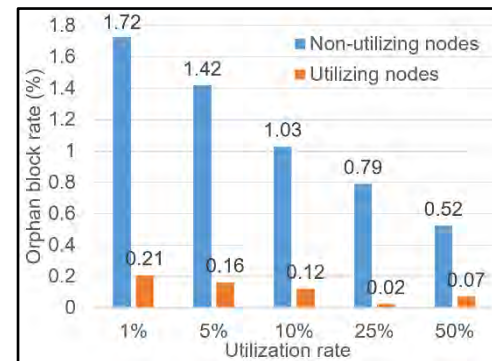
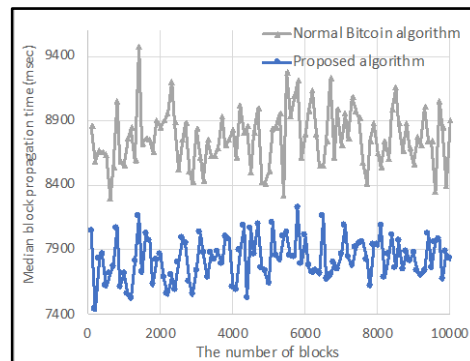
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

# シミュレータ SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019] [Shudo 2023]

- 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

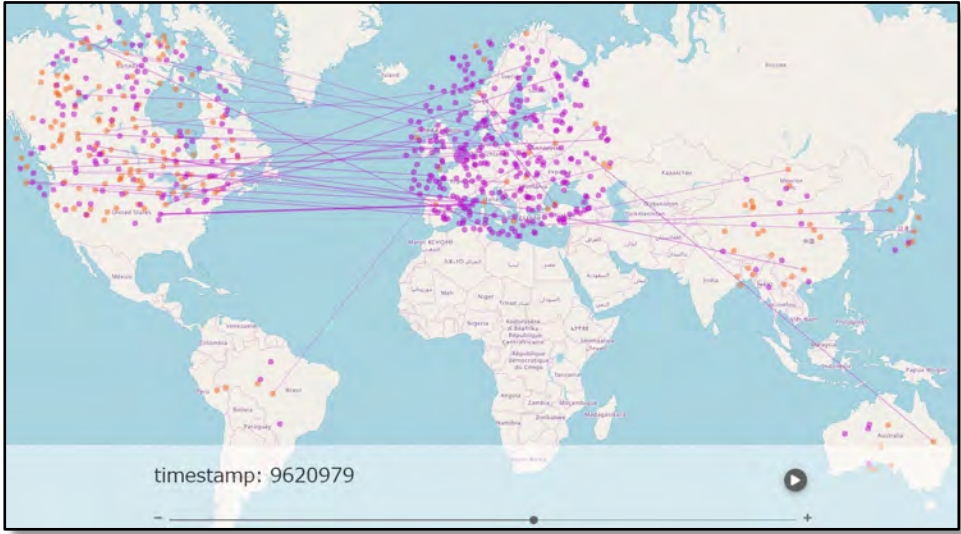
– 研究の例：



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

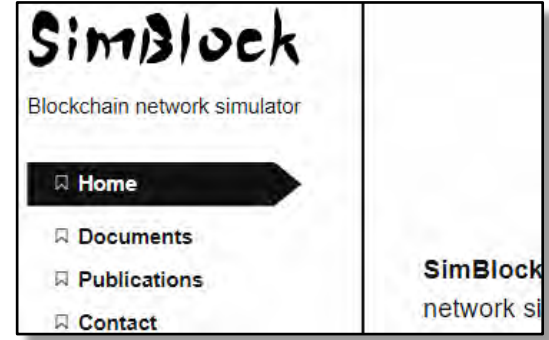
[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]



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

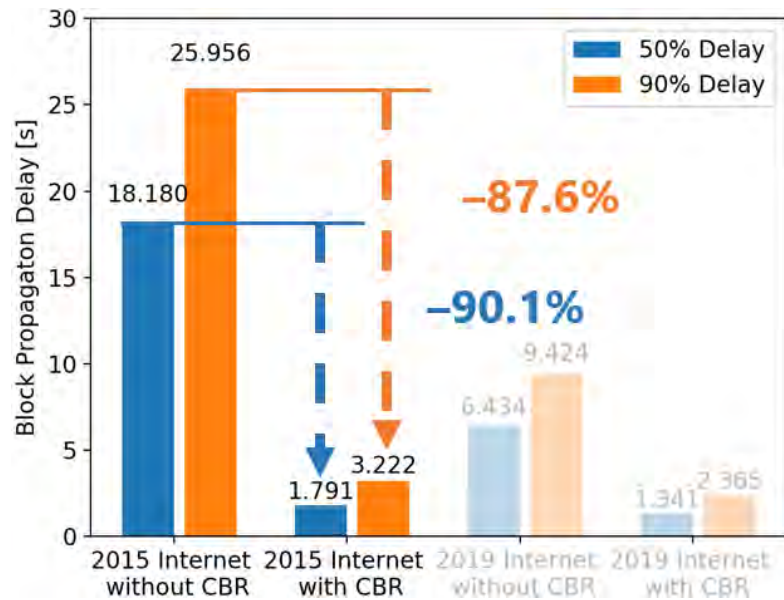
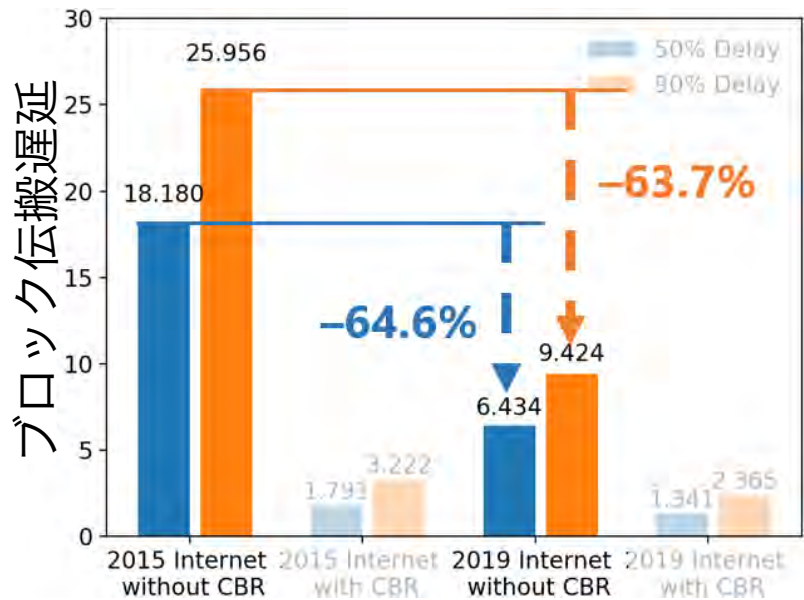
# 性能の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

# 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



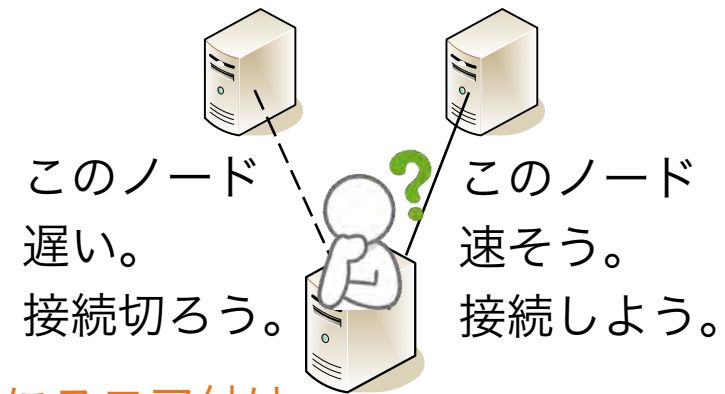
インターネット高速化 (2015→2019) の影響

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

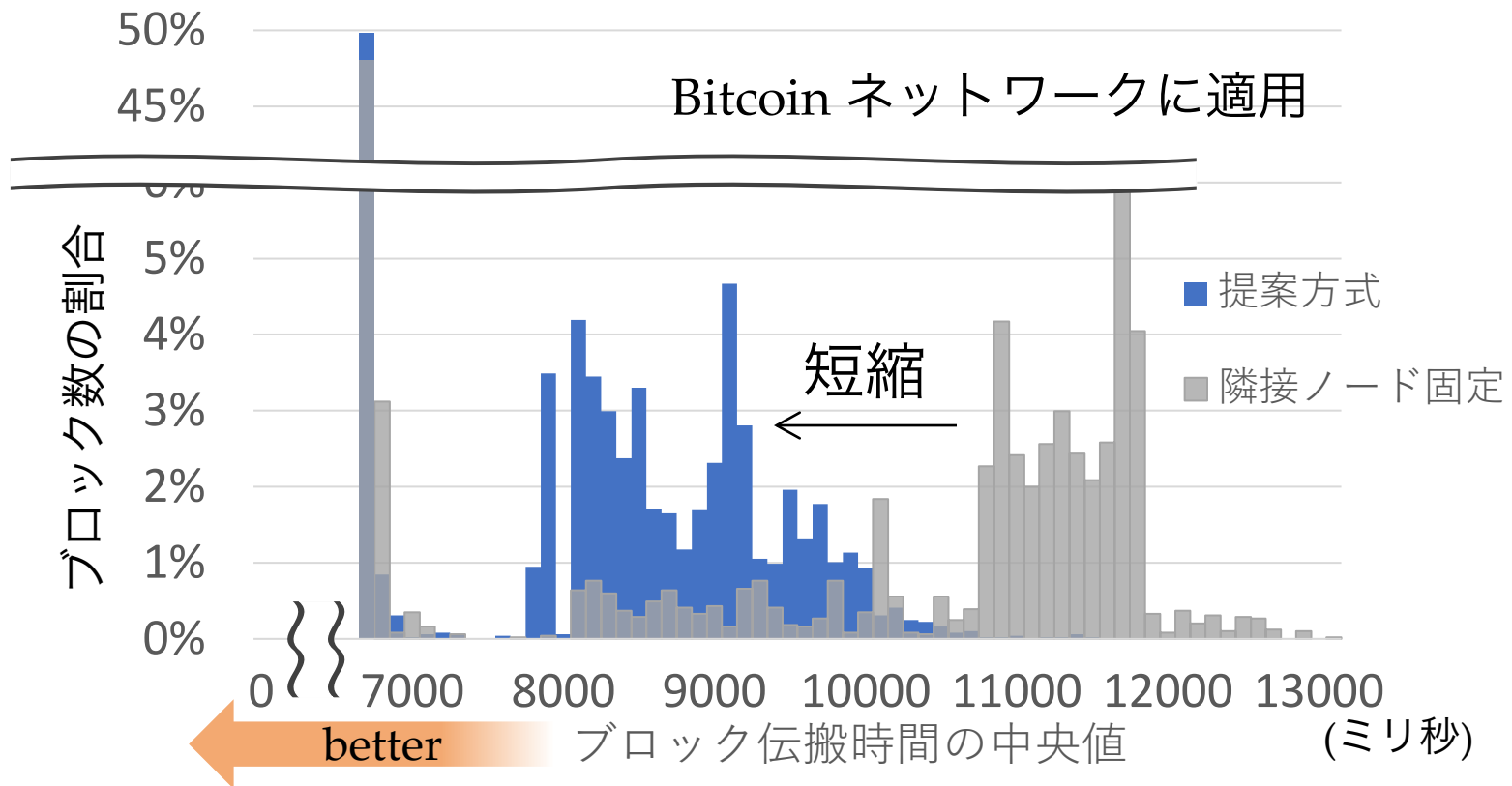
- ブロックを配信してくれた相手ノードすべてにスコア付け
  - スコア = (ブロック配信時刻 - 生成時刻) の指数重み付き平均値
- 10 ブロック受信するごとに隣接ノードを選択し直す
  - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
  - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

# 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



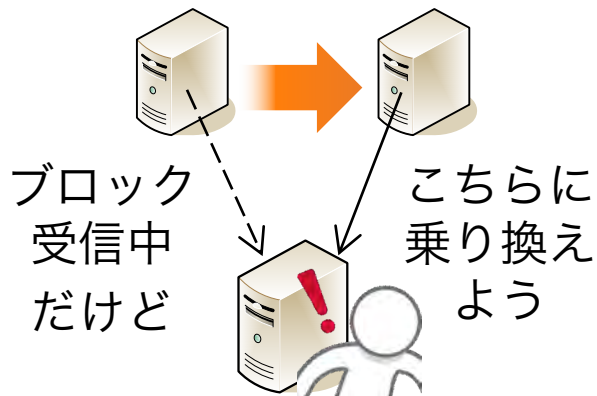
- 注：2015年のインターネットを対象として実験



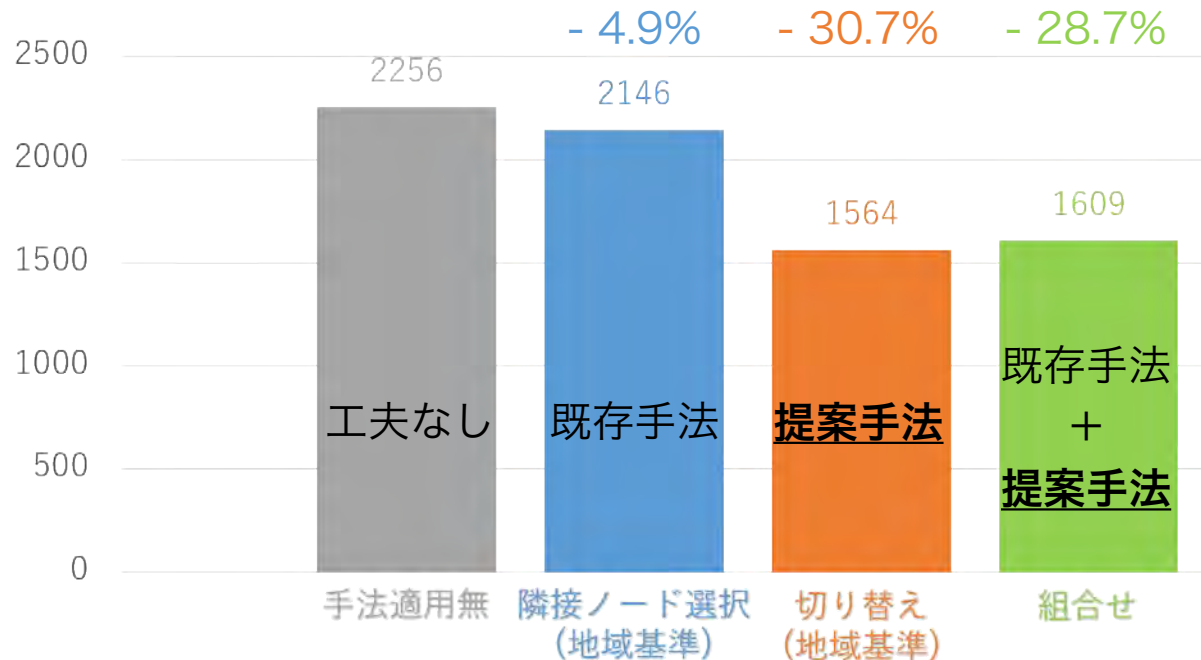
# ブロック送信元ノードの切り替え

[櫻井 2022a] [Sakurai 2023a]

- ブロック受信中でも、別ノードからの受信に切り替えてしまう。
  - 既に受信したデータは、基本的に、再度、受信する。それでも性能向上。
  - 再度の受信をしないためには、プロトコルの拡張が要る。



手法

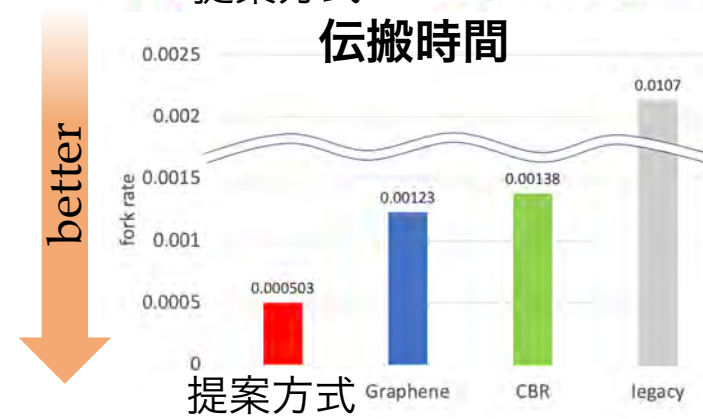
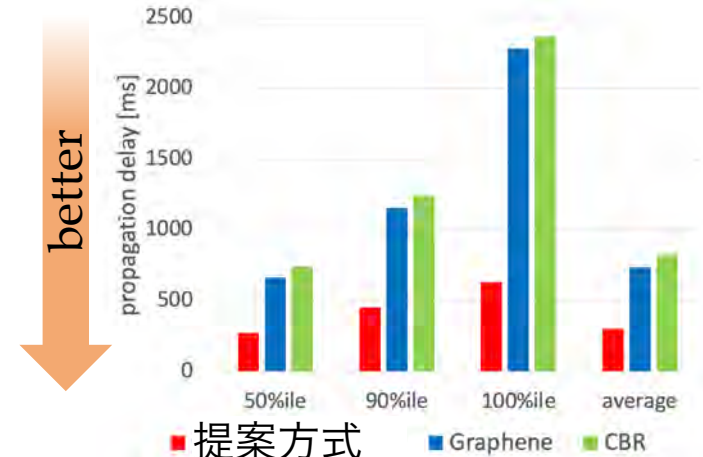
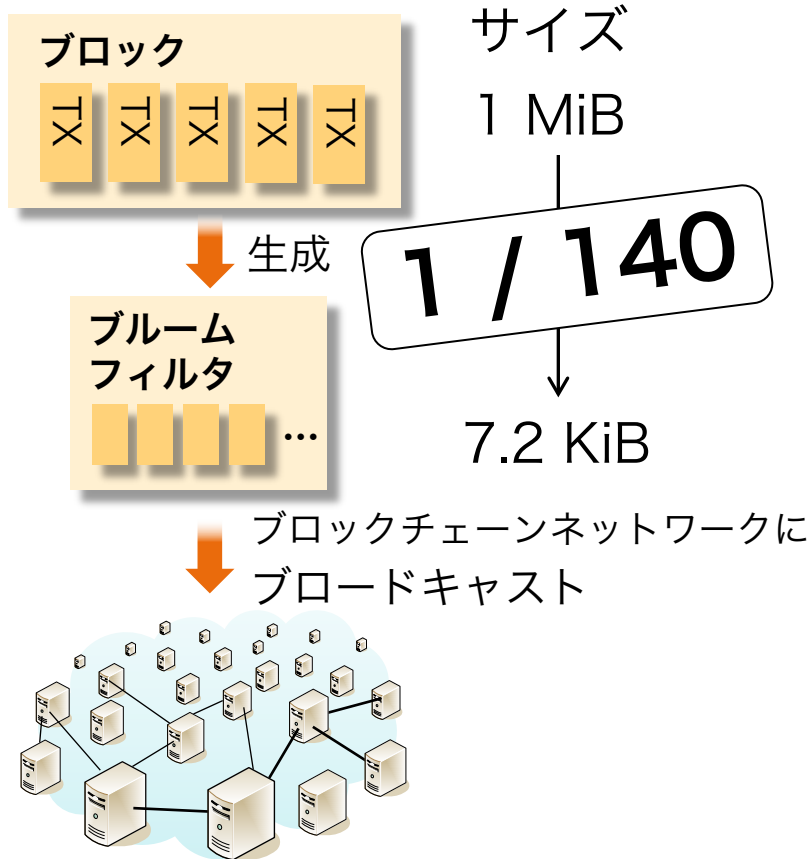


90% のノードにブロックが行き渡るまでの時間

# ブロック生成通知

[長谷川 2023a] [Hasegawa 2023b]

- ブロックの前にブルームフィルタをブロードキャストする。

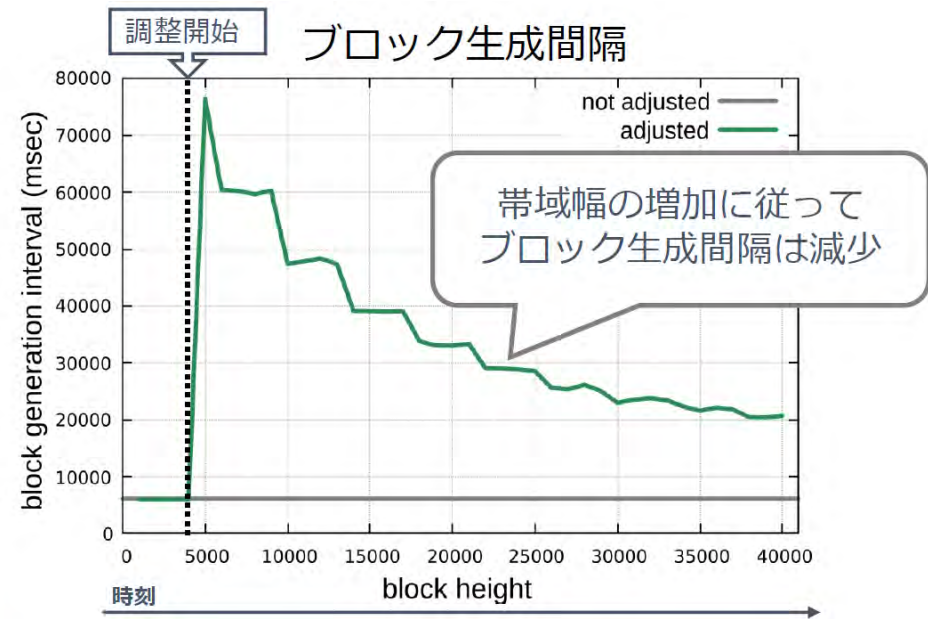
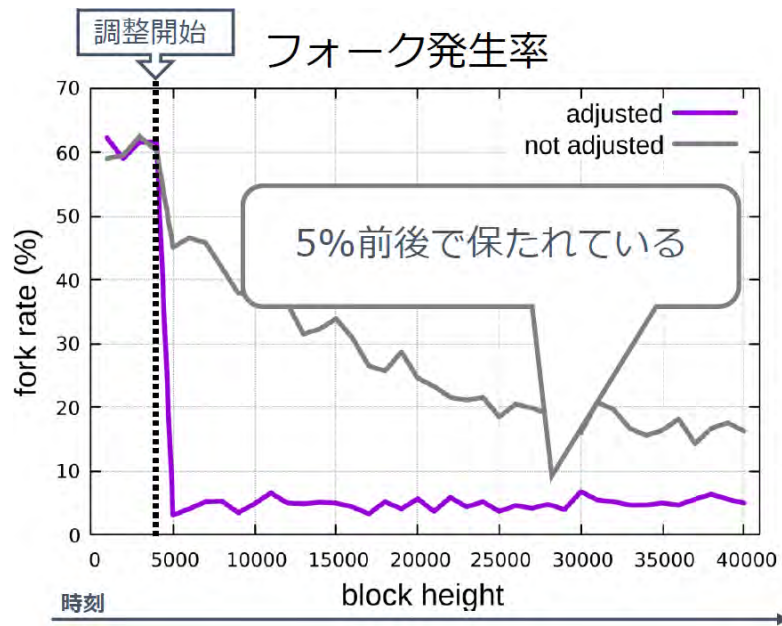


フォーク発生率 (セキュリティの指標)

# ブロック生成間隔の動的調整

[荒川 2022a] [Arakawa 2022b]

- 前提: 性能 (TPS) = ブロックあたりの TX数 / **ブロック生成間隔**
  - 当初の Bitcoin: 7 TPS = 1 MiB / 250 byte / **600 秒**
- 手法: **ブロック生成間隔を適切に縮める。**
  - セキュリティは犠牲にしない = フォーク発生率を一定に抑える
  - フォーク発生率は、一部のノード群へのブロック到着時刻から算出。



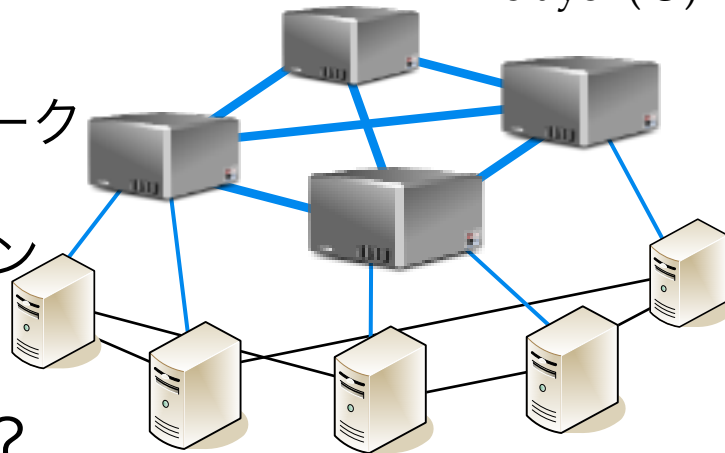
# リレーネットワーク 効果推定

[大月 2020a] [Otsuki 2020b]

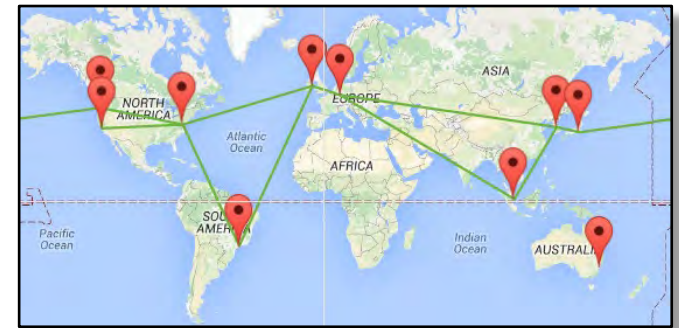
## ● リレーネットワーク

- 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 2023年時点は、Ethereum の MEV において  
relayer (も) やってる。4強の1者。

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



リレーネットワークの例: FALCON

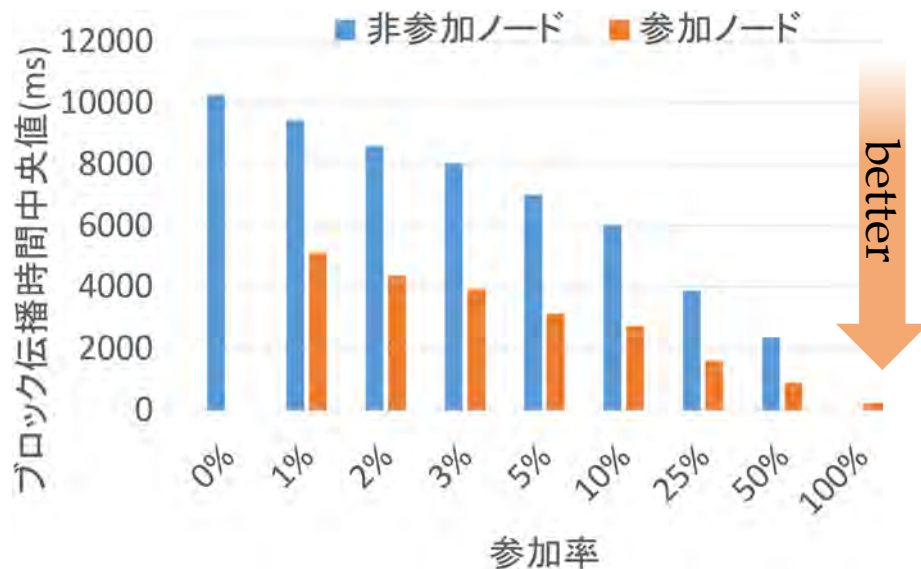
## ● 効果は？

- 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？

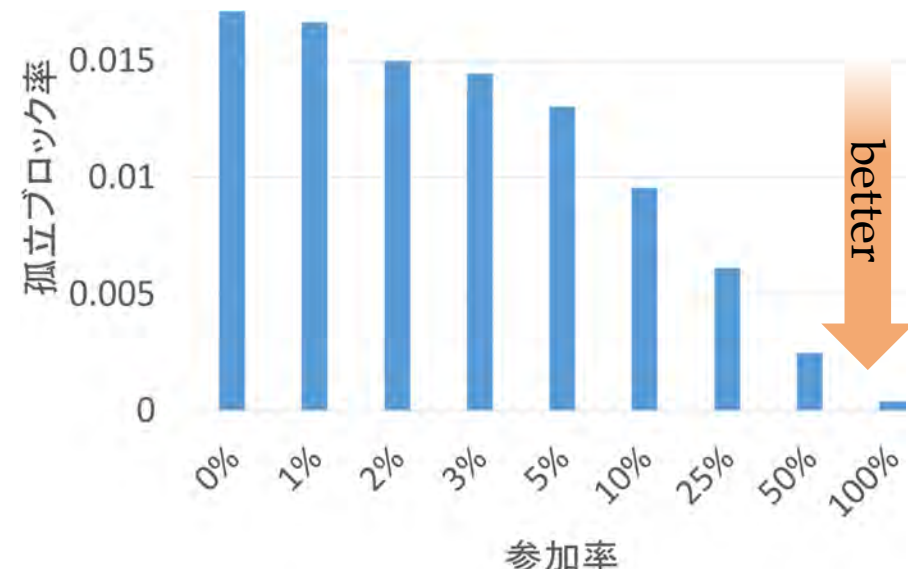
# リレーネットワーク 効果推定

[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！

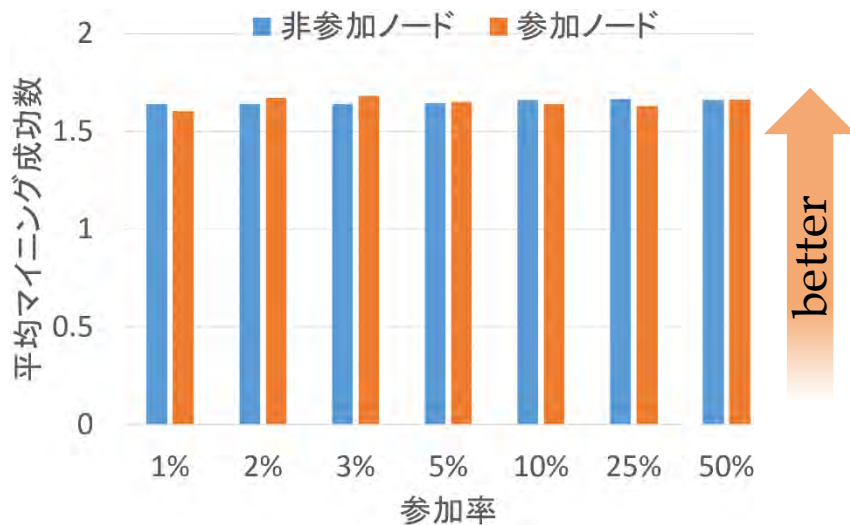
- では、ノードレベルでは？

↑  
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

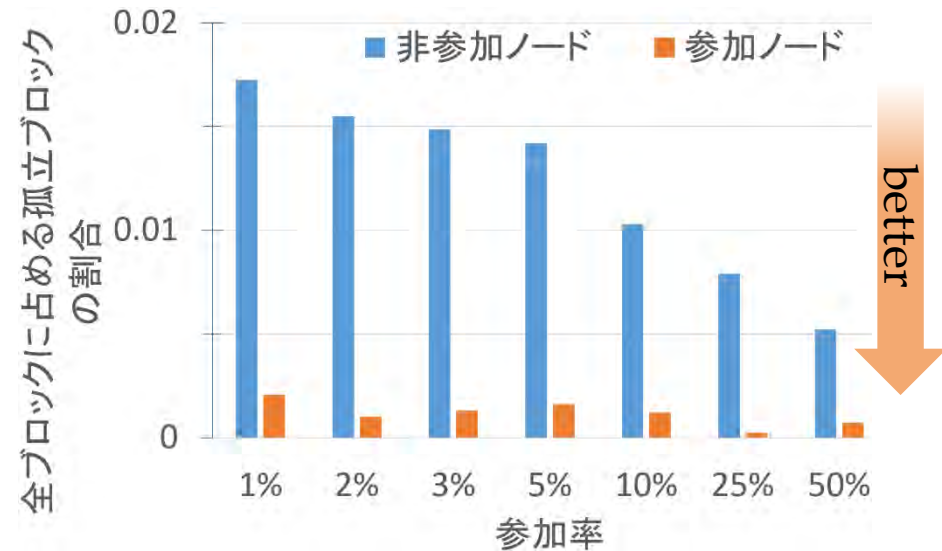
# リレーネットワーク 効果推定

[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] [北川 2022a]  
[北川 2022b] [Kitagawa 2023]

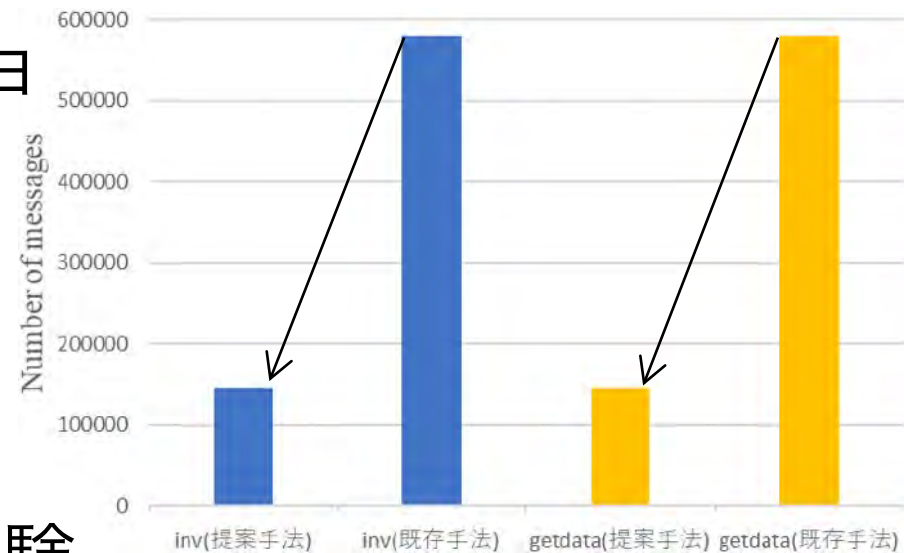
- Plumtree (IEEE SRDS 2007)

- 非構造化オーバーレイ (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
- 外部依存の削減

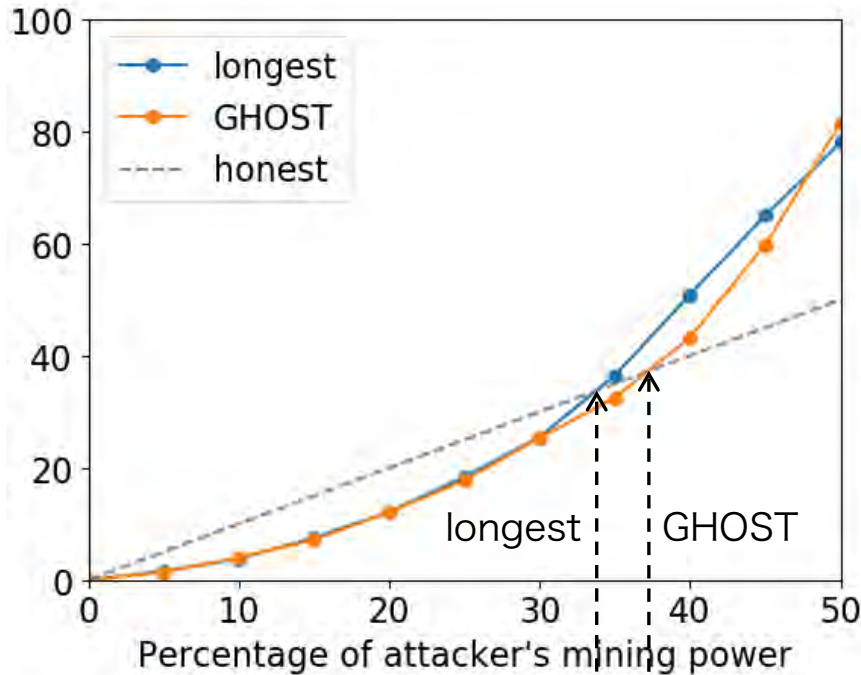


# selfish mining 攻撃を模擬

[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

メインチェーン上の  
攻撃者が生成したブロック数の割合



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]

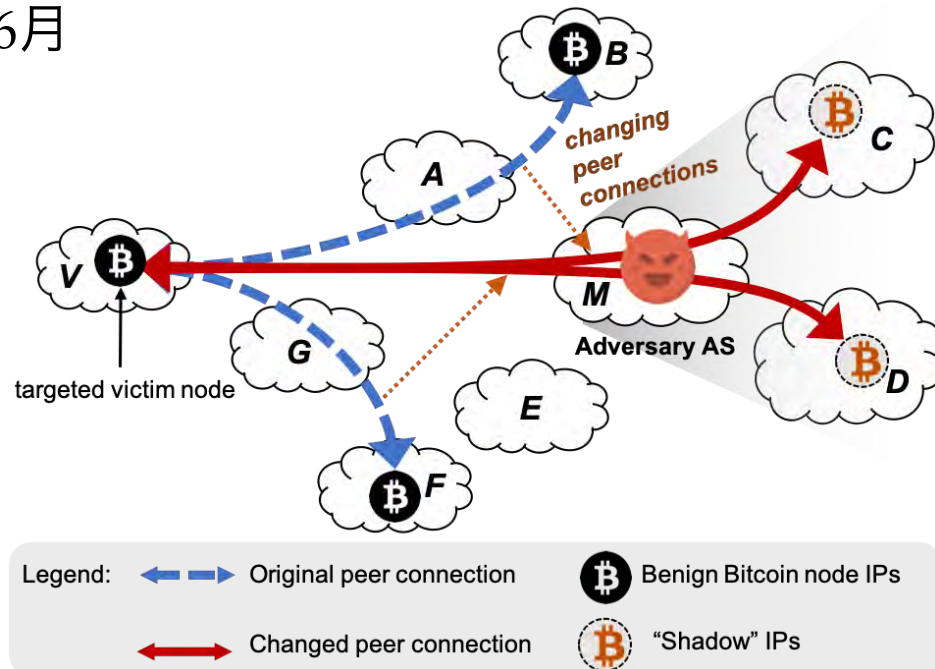
- Erebus 攻撃 (IEEE S&P 2020)
  - ネットワーク分割攻撃 → 様々な使いみち
  - AS を制御する攻撃者がノードを攻撃。  
対象ノードを攻撃者のノードに多く接続させる。

- 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。



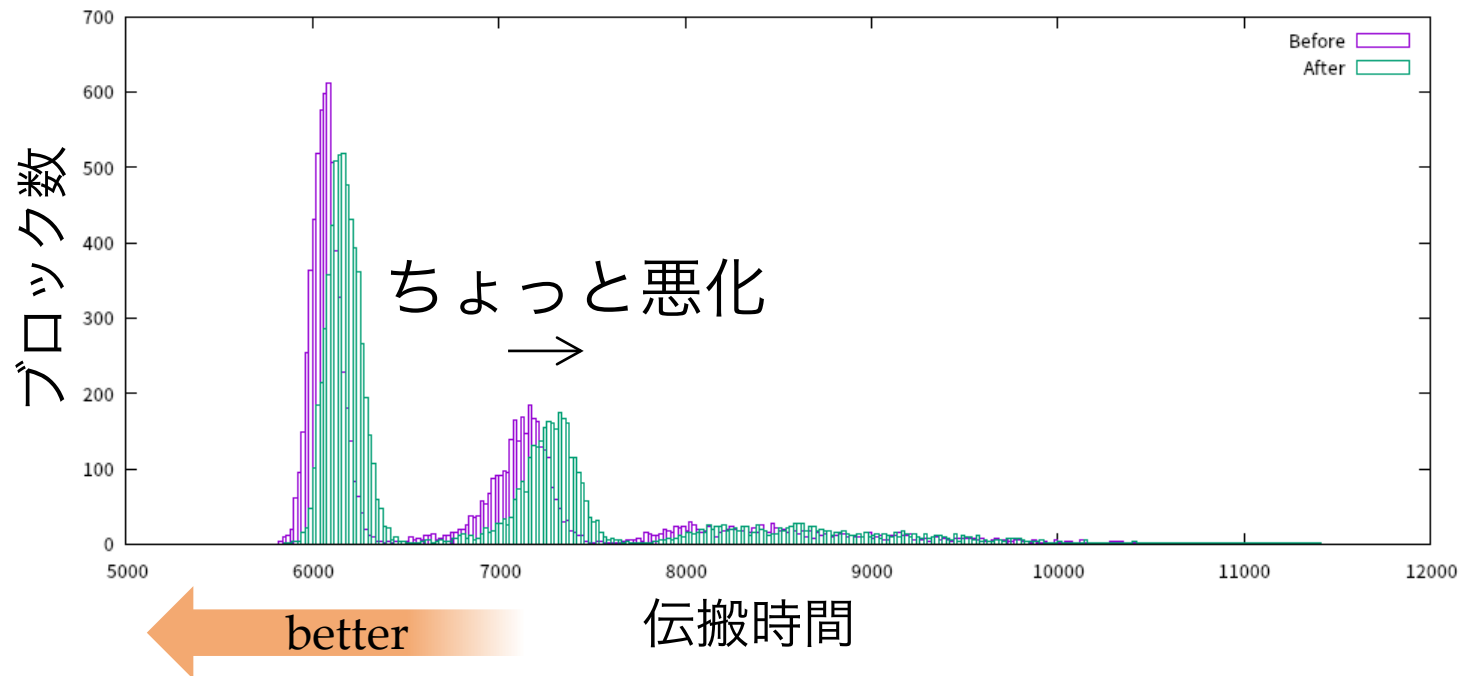
通信相手に、これまで  
なかった制約が課せられ、  
**通信性能低下？**



# 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)



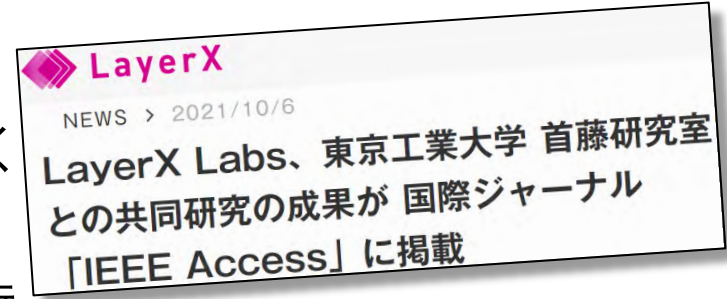
- routing 攻撃をシミュレートできた

# 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] [大月 2021b]

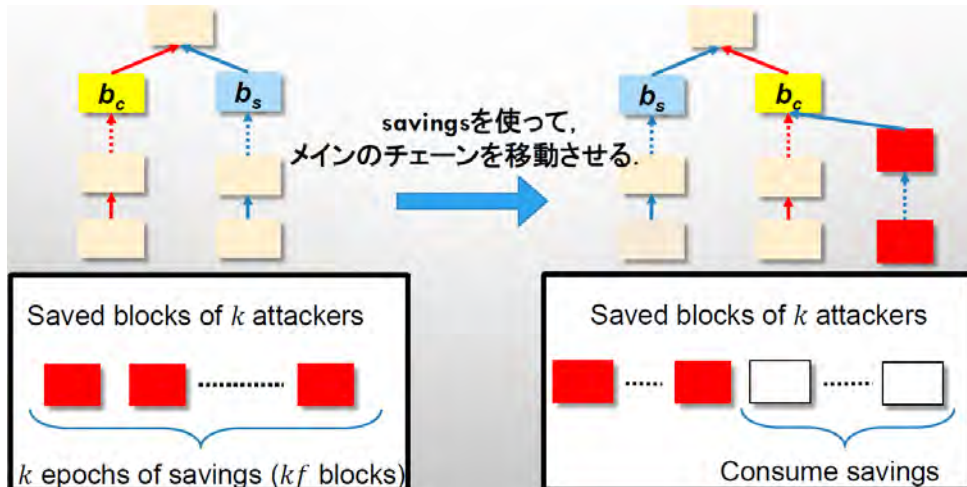
## ● saving attack を発見

- 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

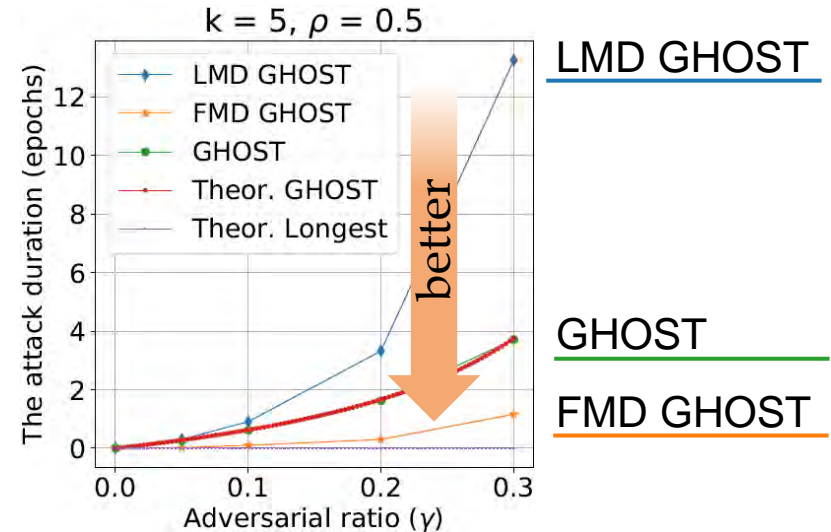


## ● メインチェーンを決める規則ごとの、攻撃への耐性を調査

- 狙った通り、FMD GHOST がベスト



saving attack



# 理論フォーク率の正確な表現

[櫻井 2022b] [Sakurai 2023a]

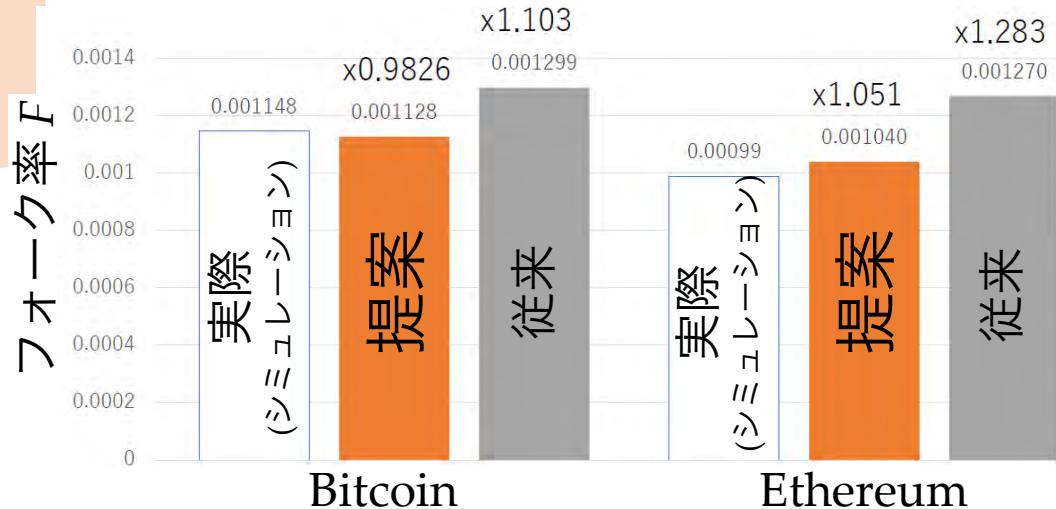
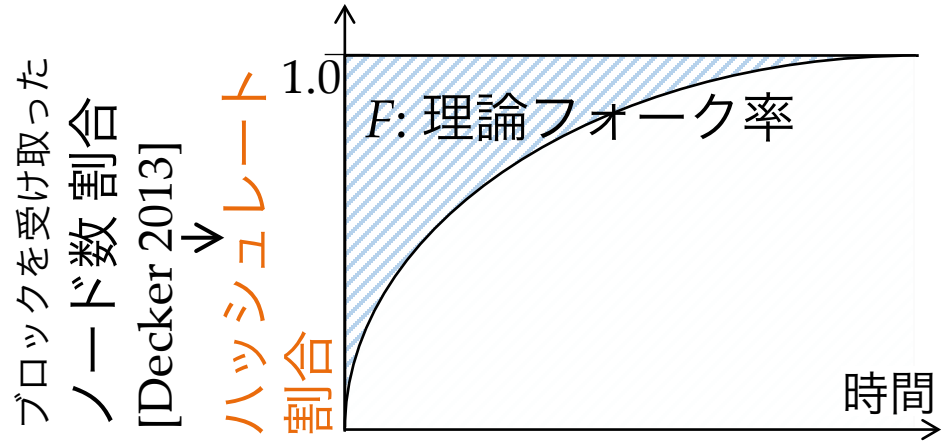
- フォーク率 (セキュリティ指標) を算出するより正確な式を提案
  - ハッシュレートを考慮


$$F = \frac{T_w \text{ (ハッシュレート重み付きブロック伝搬時間)}}{T \text{ (ブロック生成間隔 (Bitcoin は 10分))}}$$

↑  
フォーク率

- ブロックチェーンのトリレンマ (by Vitalik) (略)

「スケーラビリティ, セキュリティ, 分権化は同時には成り立たない」





# 公平性 の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

# ノード間の公平性指標と ブロック生成間隔調整

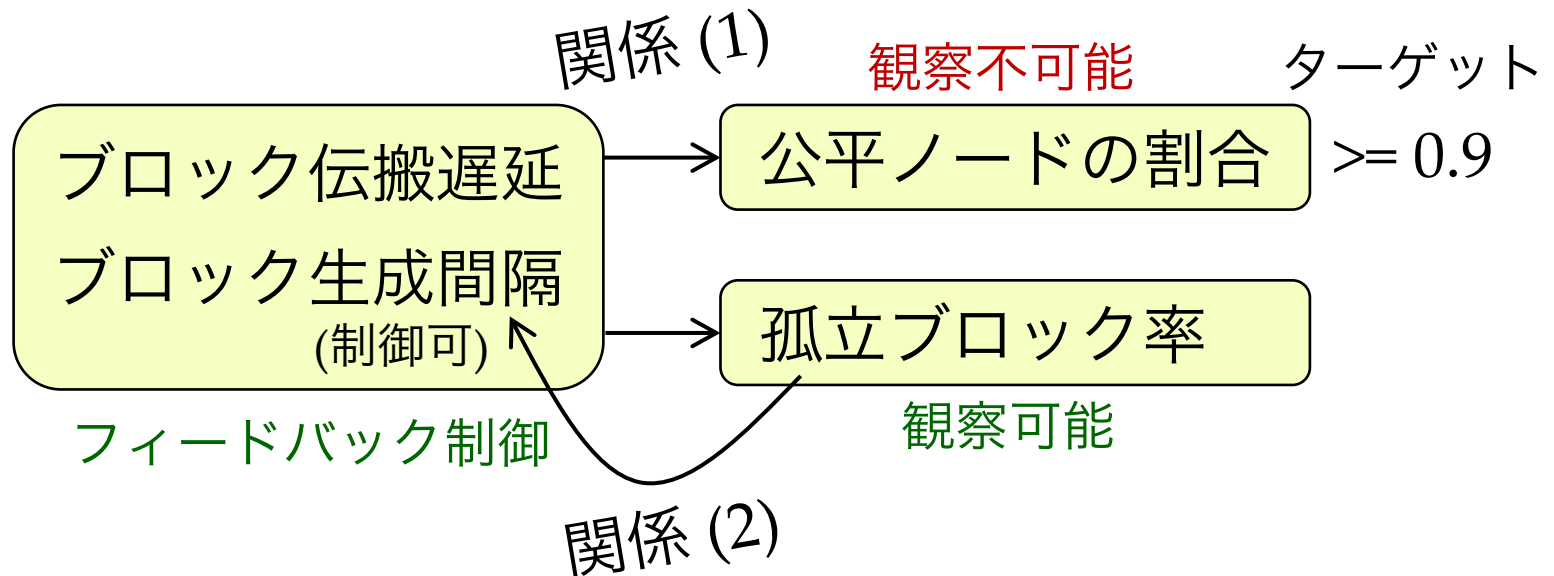
[神田 2020a]  
[Kanda 2020b]

- 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：  $(X, \varepsilon)$  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  $\varepsilon$  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。



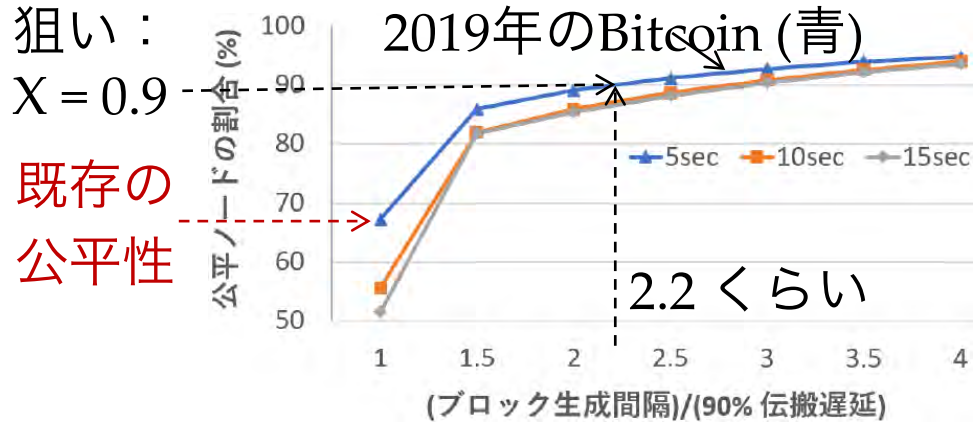


# ノード間の公平性指標と ブロック生成間隔調整

[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



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]

	ブロック生成間隔 = 2 90%伝搬遅延	ブロック生成間隔 = 3 90%伝搬遅延
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
- 外部依存の削減

# Proof of Stake 各プロトコルの 中央集権の度合い

42 / 48

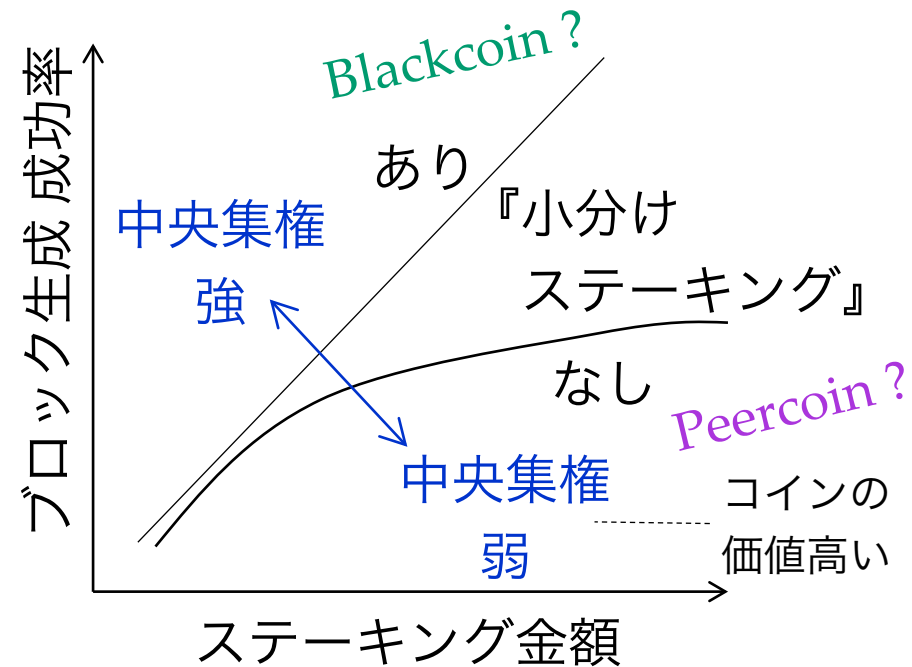
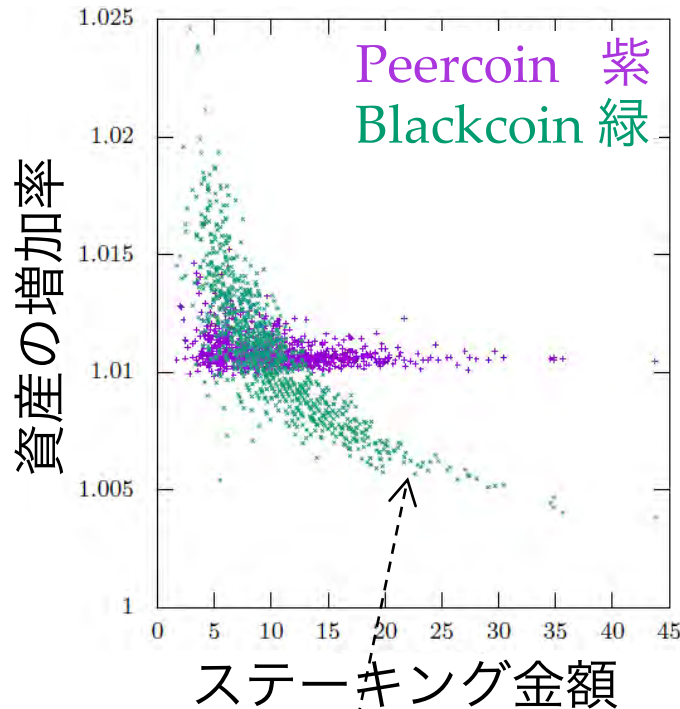
[高山 2020a]

- 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

## ● 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

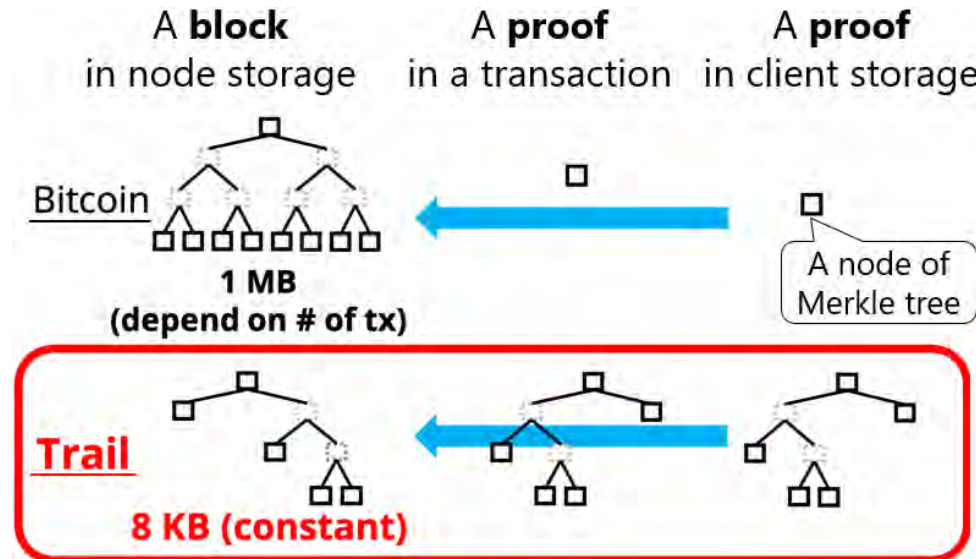
- 大きな台帳データがノード運営の負担で、  
分権化 / decentralization を妨げている。

– 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

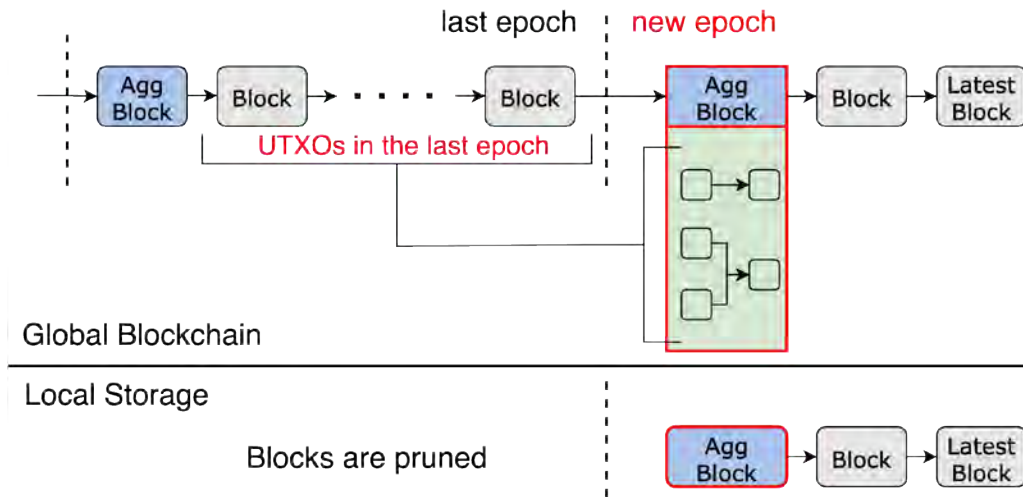
– 代わりに、クライアントが自己責任で TX を保存・バックアップ



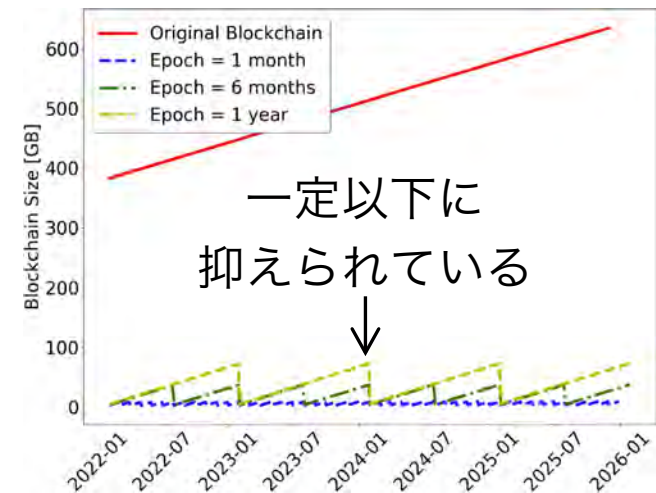
# 通常ノードが保持するデータ量を削減

[Song 2022a] [Song 2022b]


- 前提: ノードは、受信した TX・ブロックを検証する  
→ 全 UTXO を参照できるように、全ブロックを保持
- 提案: たまに **UTXO (コイン) を集約したブロック** を作る
  - ごく一部のノードは、過去の全ブロック (→ 歴史) を保存する
  - ノード群による集約のため、新しいスクリプト (命令列) を導入  
→ △ 既存 Bitcoin への導入はできず、何らかの移行措置が要る



UTXO の集約



台帳全体のサイズ



# 外部依存の削減の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化
- 外部依存の削減

# ノード群による 非集中的な 時計合わせ

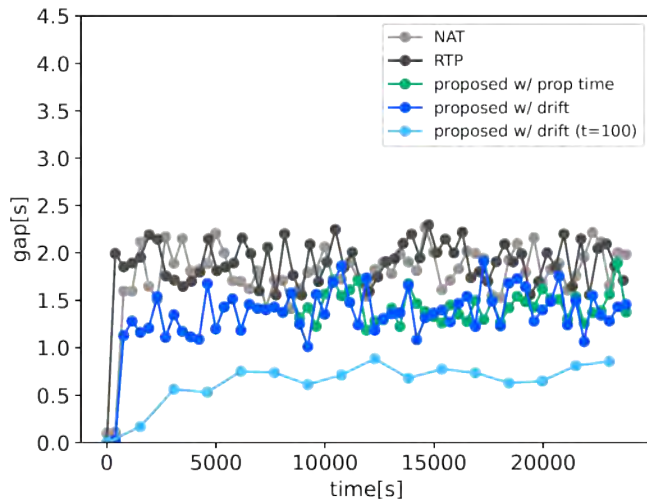
[三木 2022a] [Miki 2022b]

## ● 背景

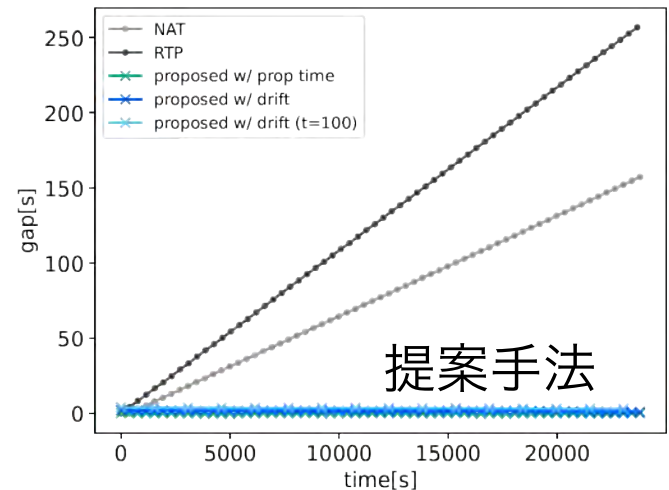
- ある種のブロックチェーン (例: Ethereum 2.0) では全ノードの時計合わせが必要
- しかし NTP や GNSS (含 GPS) に頼ることは、国家や大企業に依存すること → ノード群で時計を合わせたい

## ● 提案：ブロック伝搬のついでに皆で時計合わせ

- 新規性：伝搬の遅延を推定することで、実世界時計と離れない



提案手法

Better  
↓

提案手法

最早ノードと最遅ノードの差

実世界の時計との差



# まとめ

- ツール、性能、セキュリティ、公平性、分権化、外部依存の削減、...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終着点

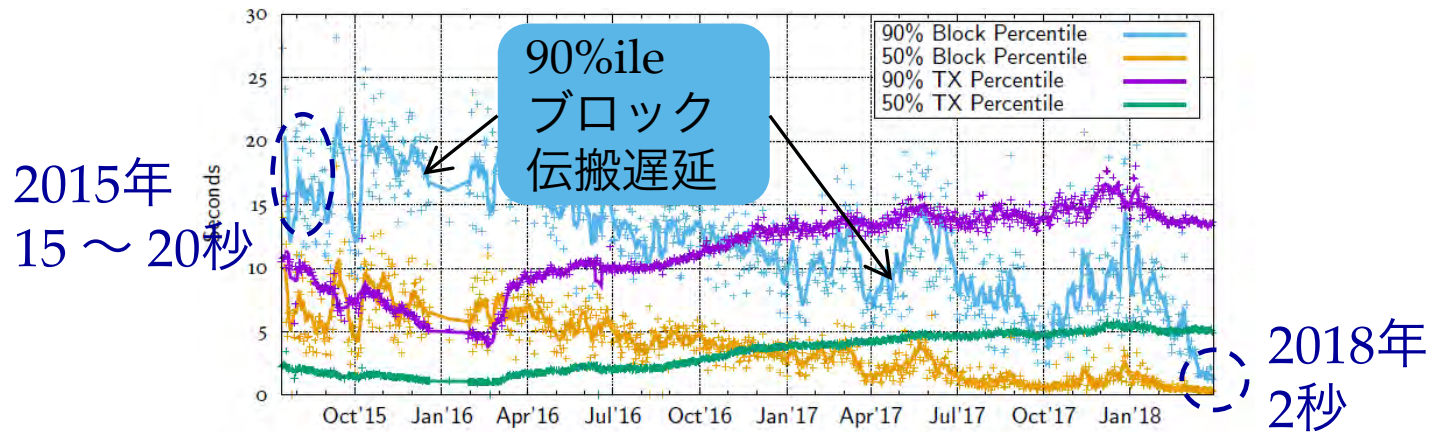


Figure 4.12: Bitcoin propagation delay for block and transaction propagation (50 % and 90 % percentiles). T. Neudecker: "Security and ...", Ph.D. thesis, 2018年

- 現在 ~ 今後：  
セキュリティ (攻撃手法と対策の考案と評価), 公平性, PoS になった Ethereum, ノードのアーキテクチャ, ...

# 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
- [Shudo 2023] Kazuyuki Shudo, Tsuyoshi Hasegawa, Akira Sakurai, Ryohei Banno: “**Blockchain Network Studies Enabled by SimBlock**”, Demonstration, Proc. 2023 IEEE Int'l Conf. on Blockchain and Cryptocurrency (IEEE ICBC 2023), 2023年 5月

# 発表 (2)

## • 性能：ブロック伝搬

- [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：ブロック伝搬 (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.10, No.8, pp.447-450, 2021年 8月 (published online on February 9, 2021)
- [櫻井 2022a] 櫻井晶, 首藤一幸: "**ブロックチェーンにおけるブロック送信元切り替えによるブロック伝搬の高速化**", 電子情報通信学会 技術研究報告, Vol.122, No.409, IA2021-67 (No.408, SITE2021-54), pp.52-57, 2022年 3月
- [Sakurai 2023a] Akira Sakurai, Kazuyuki Shudo: "**Accelerating Block Propagation with Sender Switchover in a Blockchain**", Proc. 28th IEEE Symposium on Computers and Communications (IEEE ISCC 2023), 2023年 7月
- [長谷川 2023a] 長谷川毅, 櫻井晶, 首藤一幸: "**ブロックチェーンにおけるブルームフィルタを用いたブロック生成通知の最適化**", 第15回データ工学と情報マネジメントに関するフォーラム (DEIM 2023), 2023年 3月
- [Hasegawa 2023b] Tsuyoshi Hasegawa, Akira Sakurai, Kazuyuki Shudo: "**Quick Notification of Block Generation Using Bloom Filter in a Blockchain**", Proc. 28th IEEE Symposium on Computers and Communications (IEEE ISCC 2023), 2023年 7月

# 発表 (4)

## • 性能：ブロック伝搬 (続き)

- [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
- [北川 2022a] 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 適用のシミュレーション評価**", 電子情報通信学会 技術研究報告, Vol.122, No.185, NS2022-19, pp.26-31, 2022年 9月
- [北川 2022b] 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複数 Plumtree 適用のシミュレーション評価**", 電子情報通信学会 技術研究報告, Vol.122, No.406, NS2022-204, pp.213-218, 2023年 3月
- [Kitagawa 2023] Yusuke Kitagawa, Kazuyuki Shudo, Osamu Mizuno, Ryohei Banno: "**A Study of Using Plumtree Algorithm in Blockchain Networks**", Technical Note, Journal of Information Processing (JIP), Vol.31 (2023), pp.387-391, 2023年 6月

# 発表 (5)

- 性能：ブロック生成間隔

- [荒川 2022a] 荒川真澄, 首藤一幸: "ブロックチェーンにおけるブロック伝搬時間に基づくブロック生成間隔調整", 電子情報通信学会 技術研究報告, Vol.122, No.409, IA2021-68 (No.408, SITE2021-55), pp.58-62, 2022年 3月
- [Arakawa 2022b] Masumi Arakawa, Kazuyuki Shudo: "**Block Interval Adjustment Based on Block Propagation Time in a Blockchain**", Proc. 5th IEEE Int'l Conf. on Blockchain (IEEE Blockchain 2022), 2022年 8月 (予定)

# 発表 (6)

## • 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
- [Otsuki 2021b] Kai Otsuki, Ryuya Nakamura, Kazuyuki Shudo: "**Impact of Saving Attacks on Blockchain Consensus**", IEEE Access, Vol.9, pp.133011-133022, 2021年 9月
- [櫻井 2022b] 櫻井晶, 首藤一幸: "**ブロックチェーンの理論フォーク率にハッシュレートが与える影響**", 電子情報通信学会 技術研究報告, Vol.122, No.185, IA2022-20, pp.32-35, 2022年 9月
- [Sakurai 2023a] Akira Sakurai, Kazuyuki Shudo: "**Impact of the Hash Rate on the Theoretical Fork Rate of Blockchain**", Proc. IEEE 41st International Conference on Consumer Electronics (IEEE ICCE 2023), 2023年 1月

# 発表 (7)

## • トラストレス：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

## • トラストレス：分権化 (含 ストレージ占有量の低減)

- [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
- [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
- [Nagayama 2022] Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo: "**Trail: An Architecture for Compact UTXO-Based Blockchain and Smart Contract**", IEICE Transactions on Information and Systems, Vol.E105-D, Issue.2, pp.333-343, 2022年 2月
- [Song 2022a] Song Taegy, 首藤一幸: "**UTXO AggregationによるBlock Pruning**", 第14回データ工学と情報マネジメントに関するフォーラム (DEIM 2022), 2022年 2月
- [Song 2022b] Taegy Song, Kazuyuki Shudo: "**Block Pruning With UTXO Aggregation**", Proc. 5th IEEE Int'l Conf. on Blockchain (IEEE Blockchain 2022, BlockchainEvo 2022), 2022年 8月



# 発表 (8)

## ● トラストレス：外部依存の削減

- [三木 2022a] 三木友弥, 首藤一幸: "**Proof of Stakeブロックチェーンにおける分散時刻同期プロトコル**", 電子情報通信学会 技術研究報告, Vol.122, No.85, IA2022-2 (No.86, ICSS2022-2), pp.8-14, 2022年 6月
- [Miki 2022b] Yuya Miki, Kazuyuki Shudo: "**A Distributed Clock Synchronization Protocol for Proof of Stake Blockchains**", Proc. 5th IEEE Int'l Conf. on Blockchain (IEEE Blockchain 2022), 2022年 8月

## ● 応用

- [高山 2021a] 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
- [Takayama 2021b] Shu Takayama, Yuto Takei, Kazuyuki Shudo: "**An Examination Protocol for Handling Programmable Answers Using a Public Blockchain**", Proc. 4th IEEE Int'l Conf. on Blockchain (IEEE Blockchain 2021, IEEE Workshop on Blockchain Security, Application, and Performance (BSAP 2021)), pp.361-368, 2021年 12月