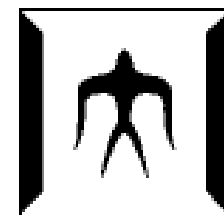


ブロックチェーン「ネットワーク」 の研究

首藤 一幸
東京工業大学

SimBlock

bit.ly/DPS-185-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



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, 商用実績

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

著者5人, 1万数千部

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 ~

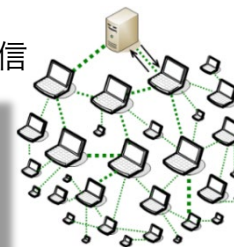
1億ノード / 10台, 既存手法の20倍の性能, Apache Spark 上

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 ~

Overlay
Weaver



魔法のようなソフト

大規模
分散システム

2020年 12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

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 37兆円 「通貨」になりたいが現状「資産」

3,000 種類以上ある



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.

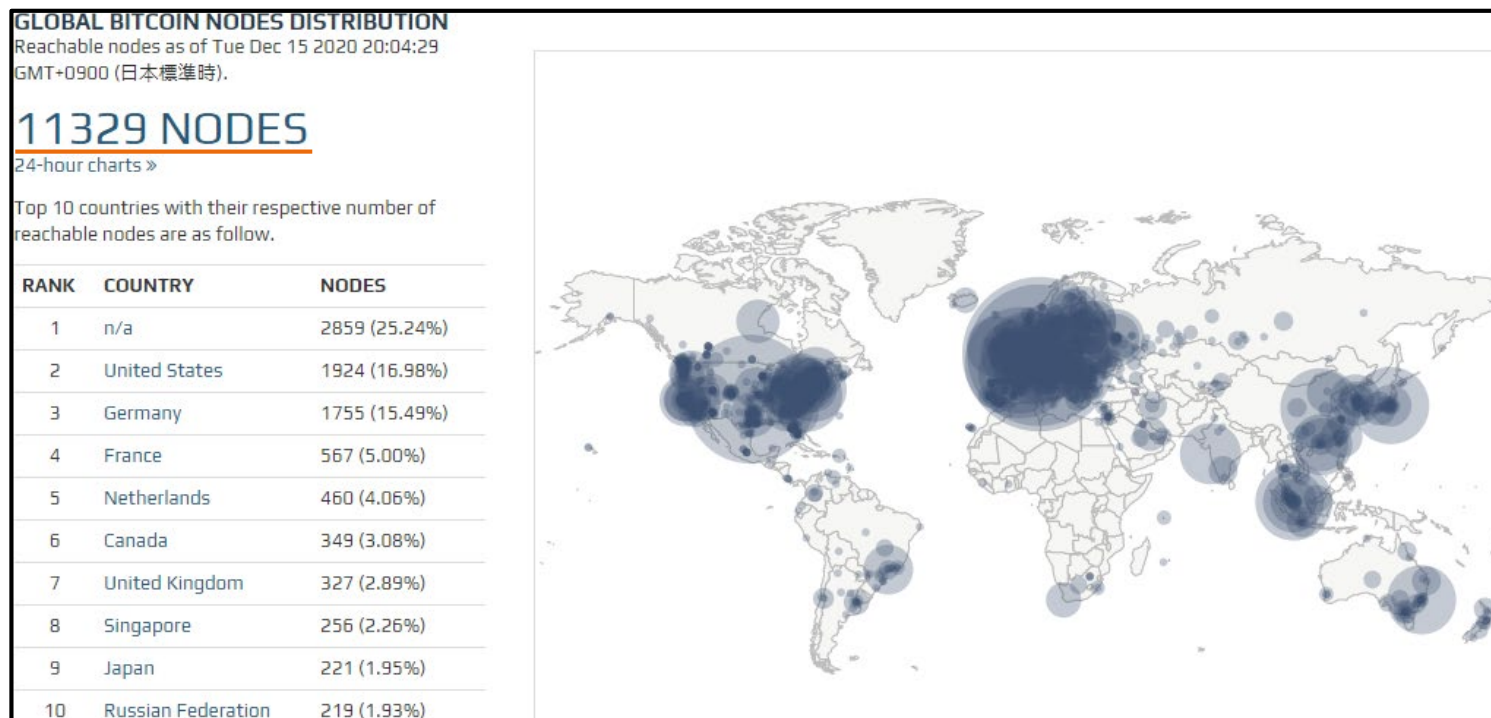
See bitcoin.org for screenshots.

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



<http://bitnodes.earn.com/> より

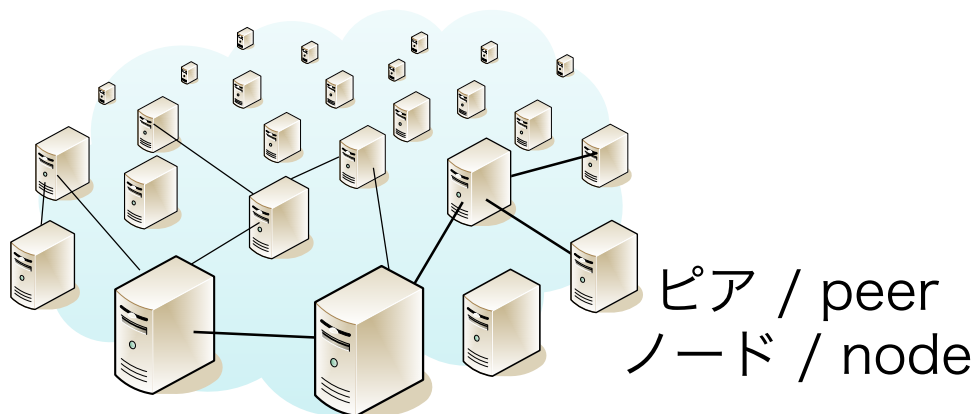
- **非集中** → 一部壊れても全体は動作し続ける

トラストレス / trustless

- 非集中 / decentralized



- 誰かを信用する必要がない → 「**trustless**」
トラストレス
 - 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。



非集中 分散システム (peer-to-peer)

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

 ● **整合性** を保つ  **トレーサビリティ**
consistent 整合性確認のために traceability
(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」の研究を踏まえ、「セキュリティ」の研究を開始
- パブリックブロックチェーンに強く期待されている「分権化」(⇔集中)、および、社会を支える基盤として必要な「公平性」の研究に着手

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]



相互に影響

性能

含 実時間性・スケールアウト性

[神田 2019a]

伝搬時間 推定 [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]



研究手段を提供



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]

分権化 / decentralization

[高山 2020a]

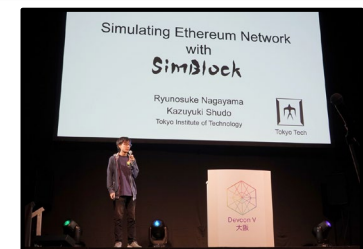
中央集権の度合い評価

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]

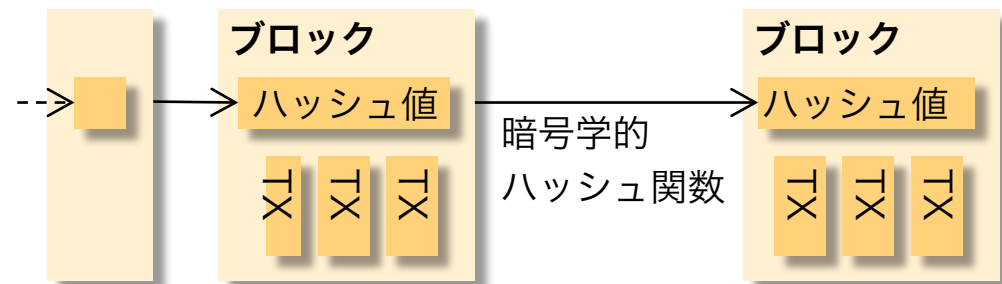
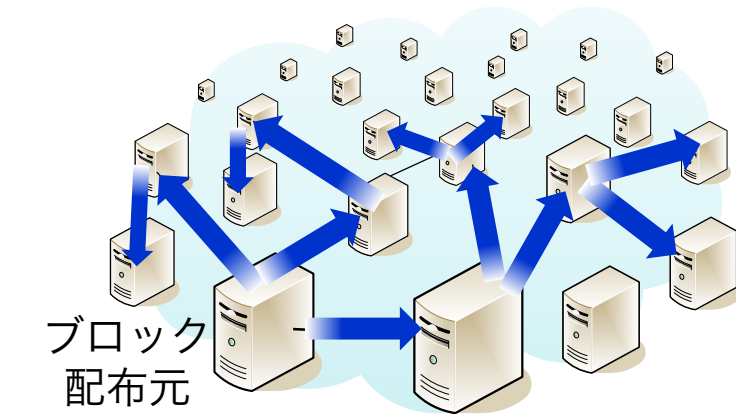


性能の研究

- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

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

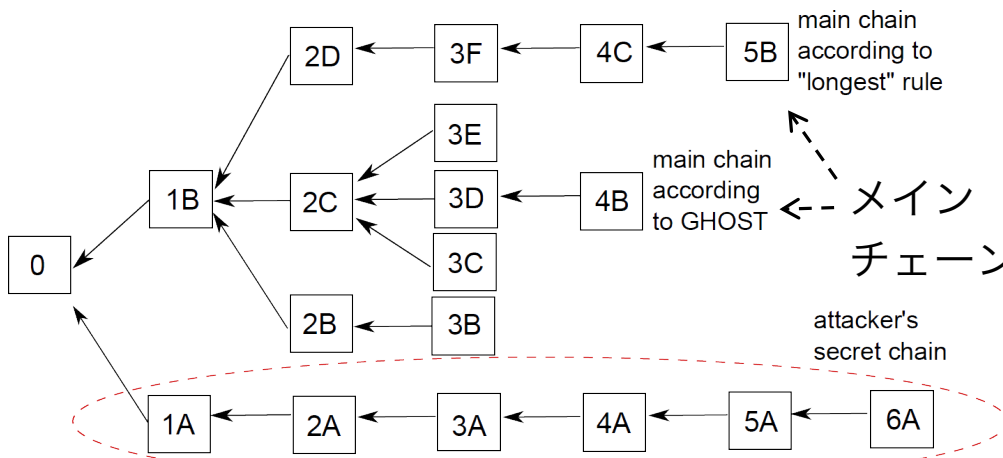
ブロックチェーンが用いるデータ構造

ノード間で、ブロックを伝搬させ、行き渡らせる

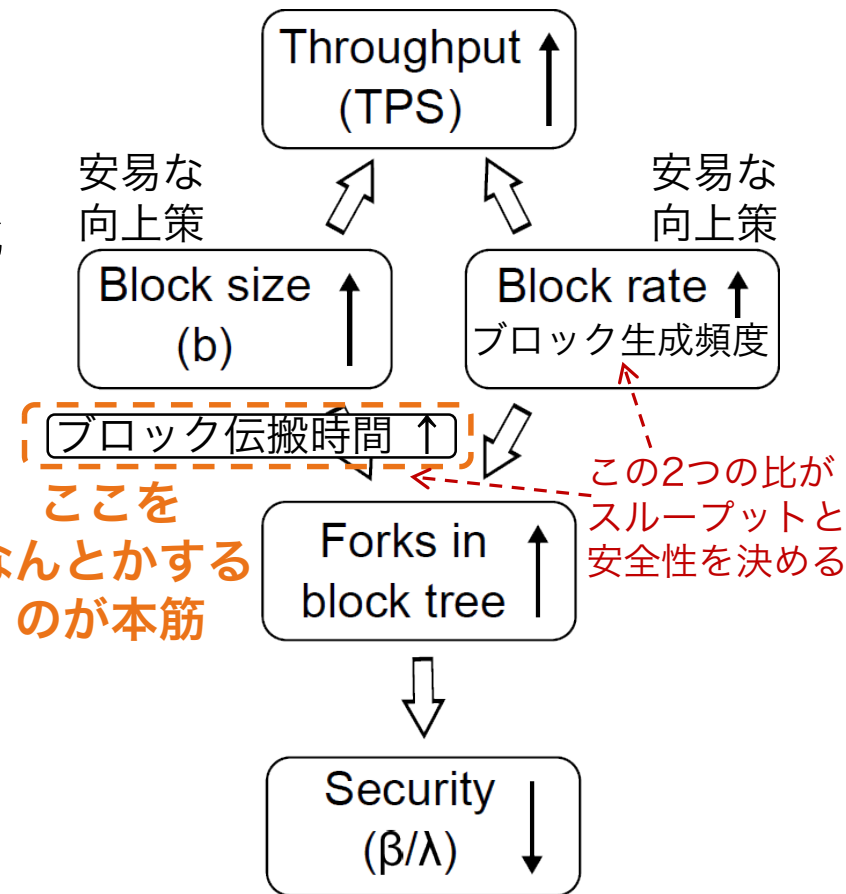
性能向上 vs. 安全性

• 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



伝搬時間 推定 with ネットワーク座標系

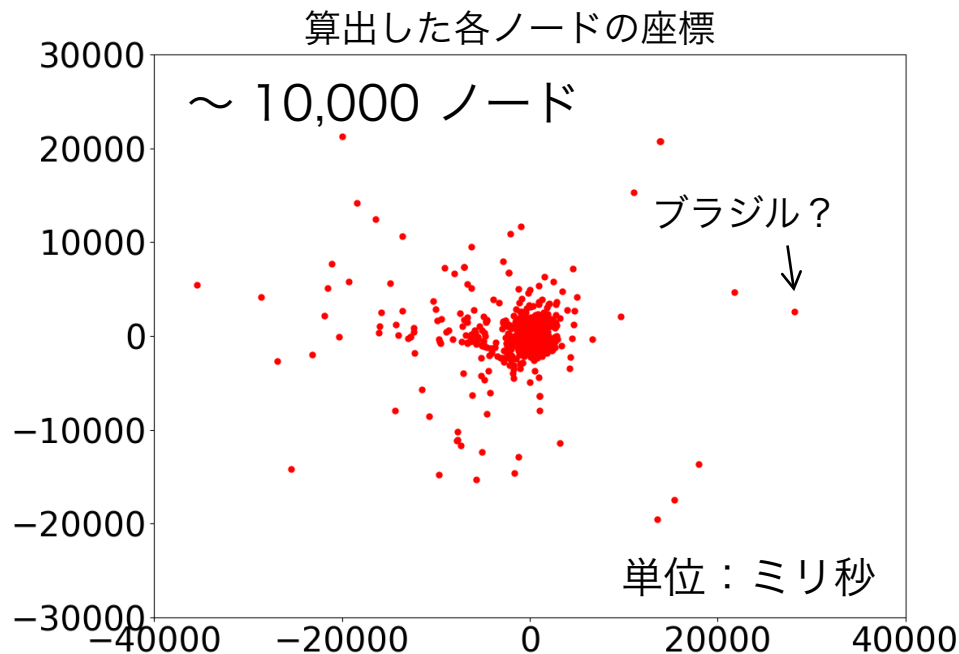
15 / 39

[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

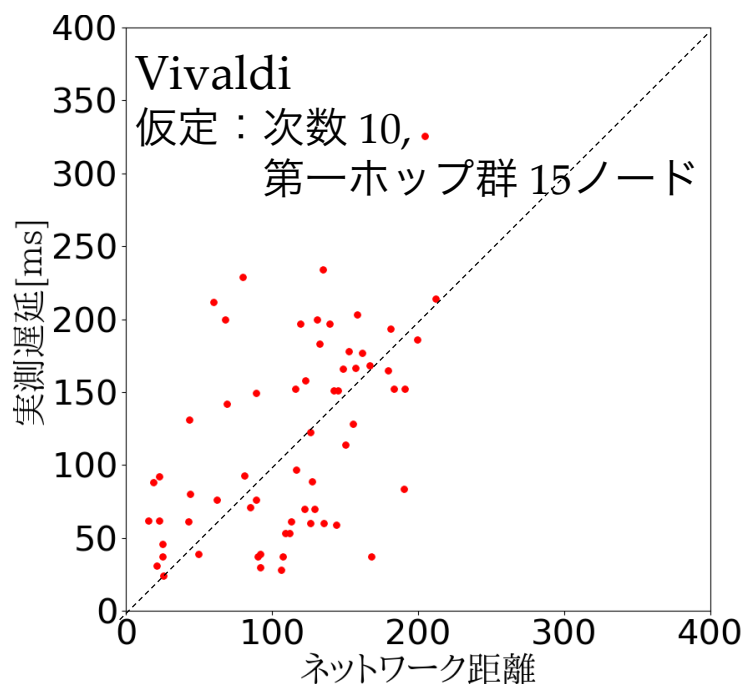
- ただ...

伝搬時間 推定 with ネットワーク座標系

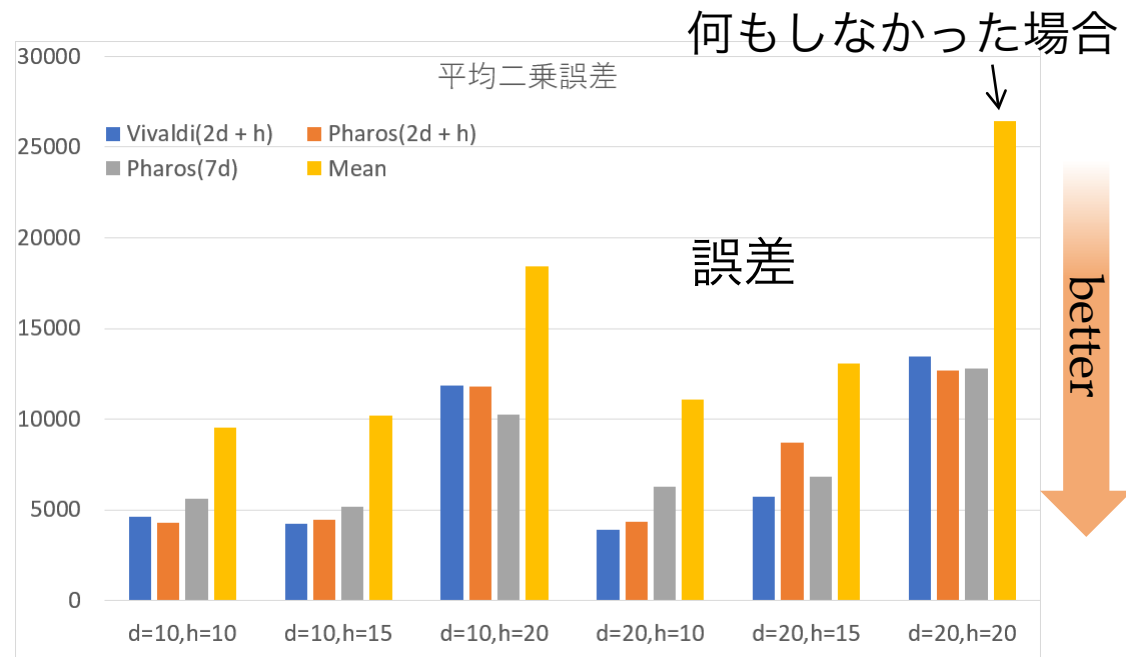
16 / 39

[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

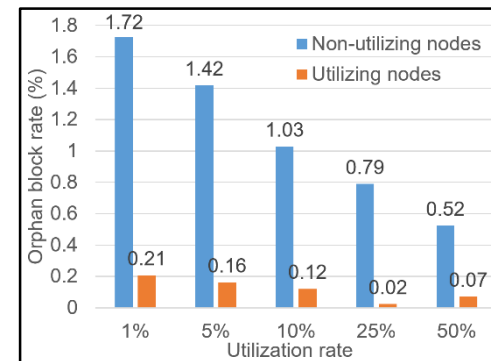
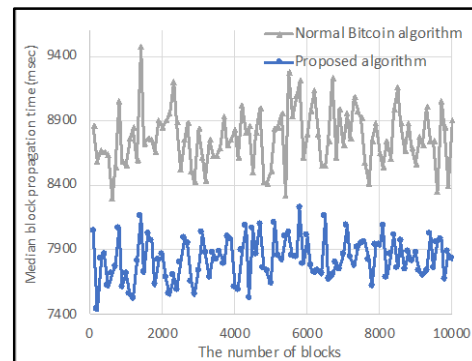
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

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

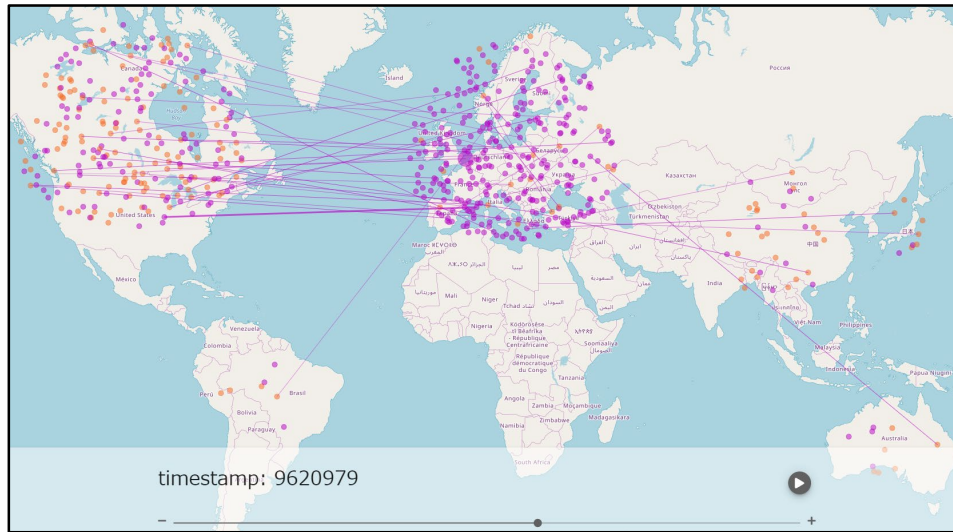
– 研究の例：



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]



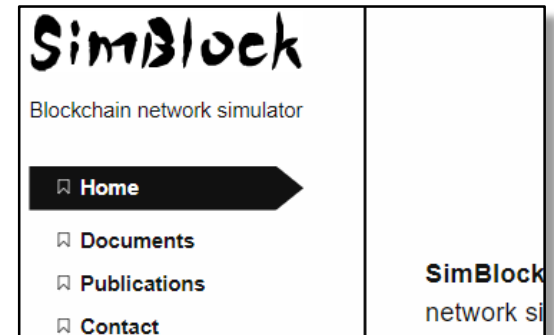
Visualizer

縮小 Bitcoin ネットワーク,
600 ノード



IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

ウェブ
サイト



IEEE Spectrum
記事



再び 性能の研究

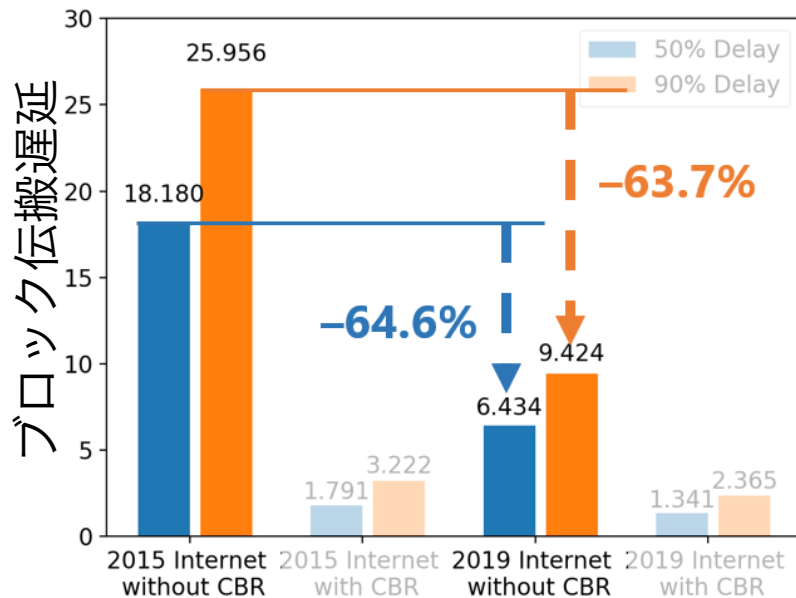
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

インターネット高速化と Compact Block Relay の影響

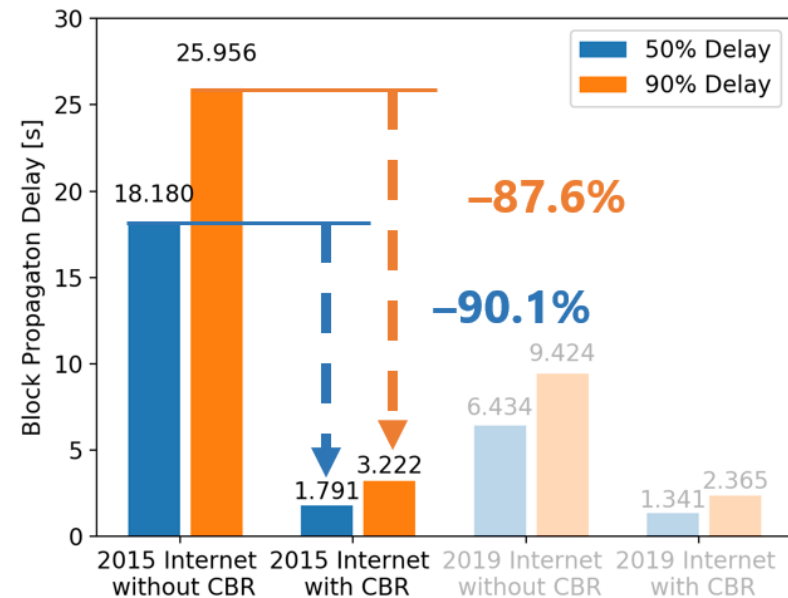
[永山 2020a]

[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



<



better

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

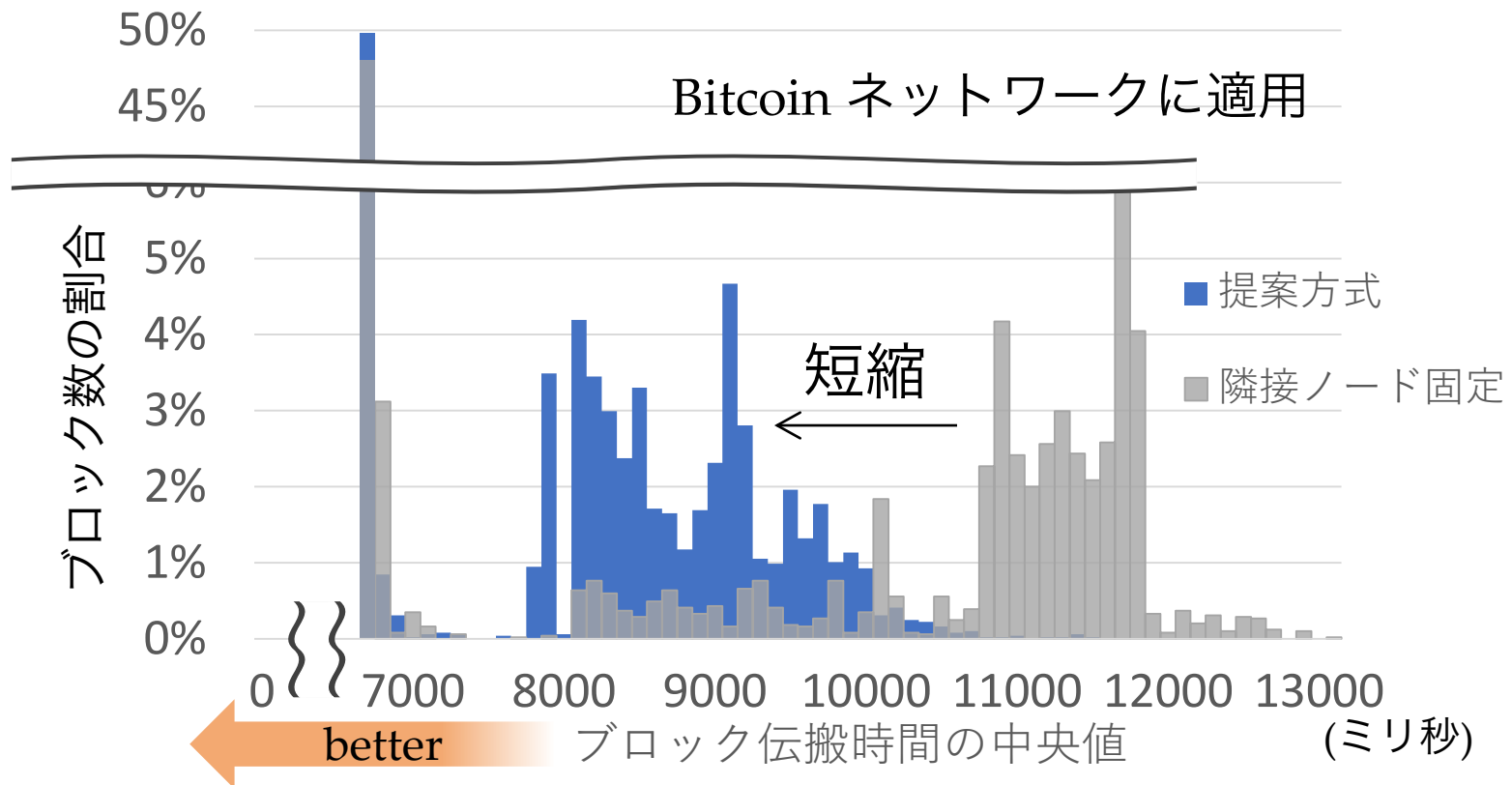


隣接ノード選択

[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



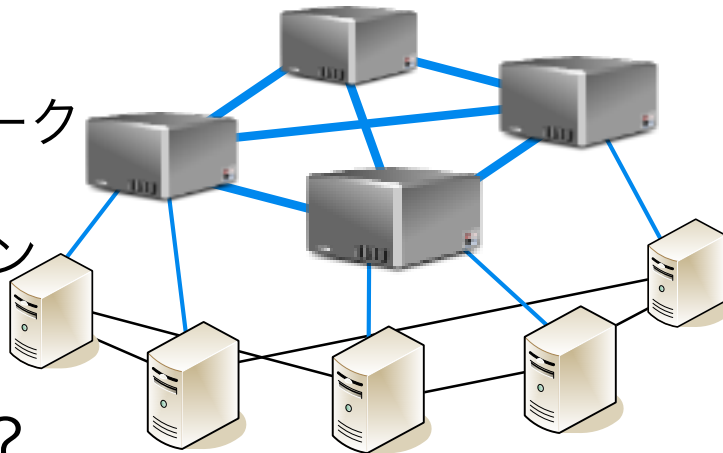
- 注：2015年のインターネットを対象として実験

リレーネットワーク 効果推定

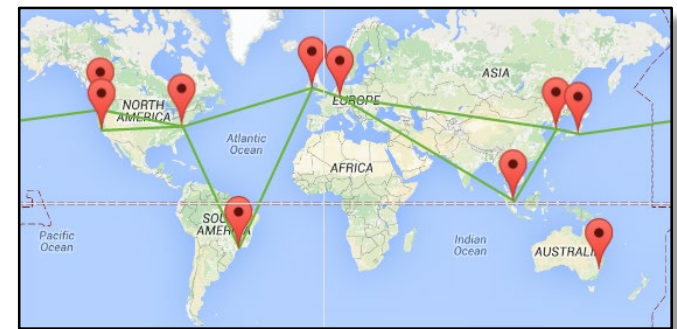
[大月 2020a] [Otsuki 2020b]

- 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



通常の
ブロックチェーン
ネットワーク



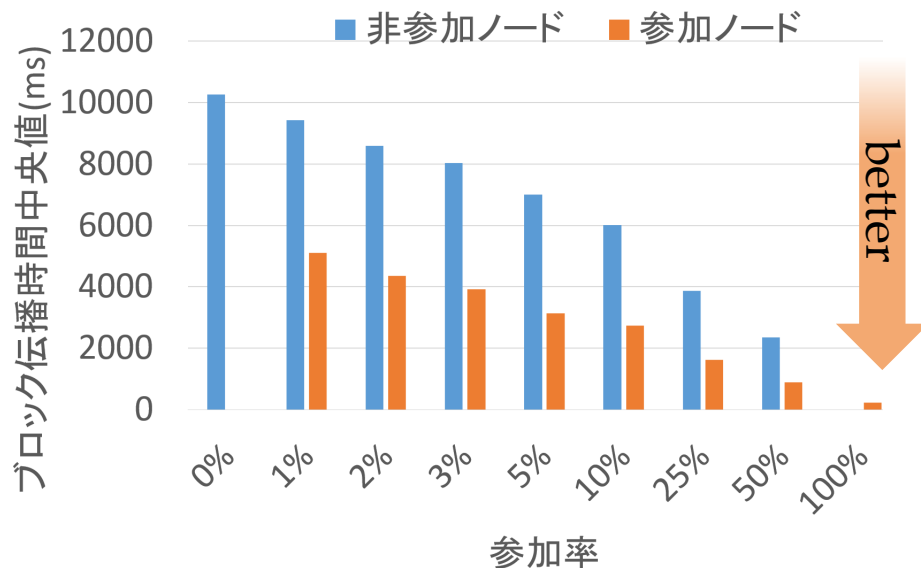
リレーネットワークの例: FALCON

- 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？

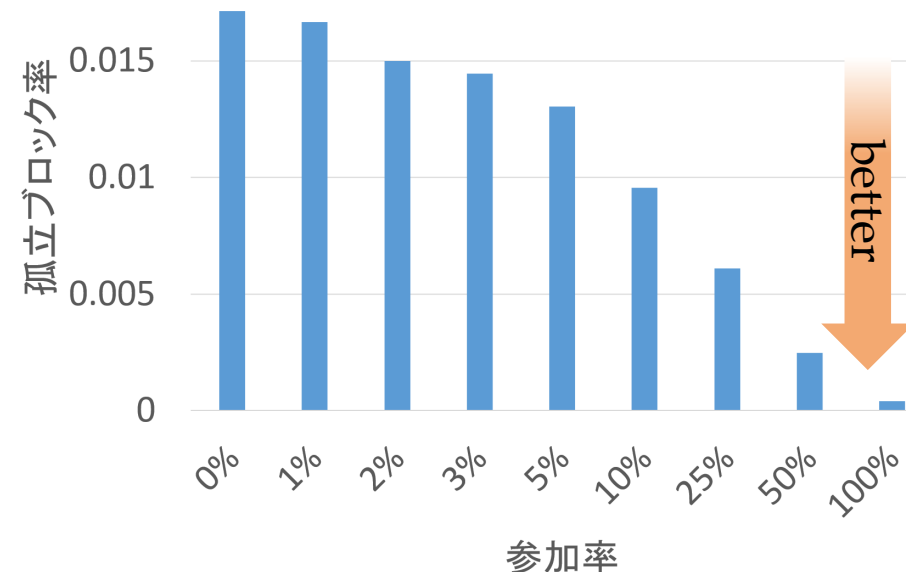
リレーネットワーク 効果推定

[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！

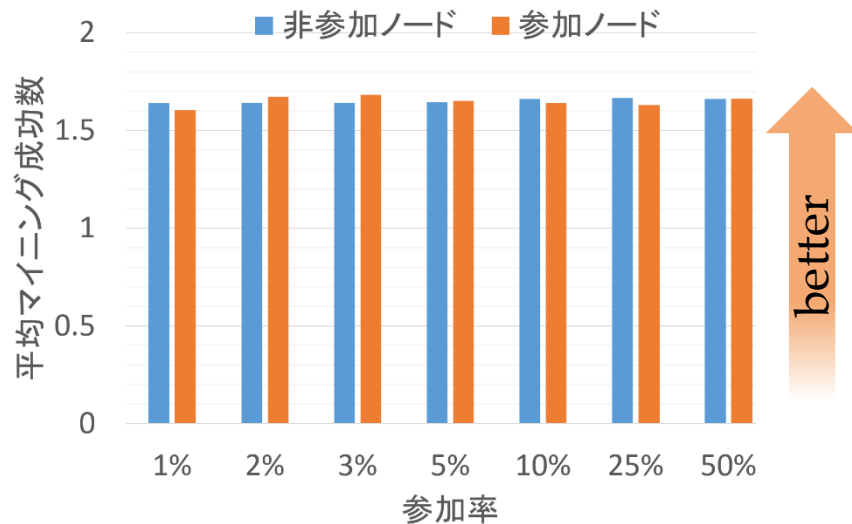
- では、ノード レベルでは？

↑
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

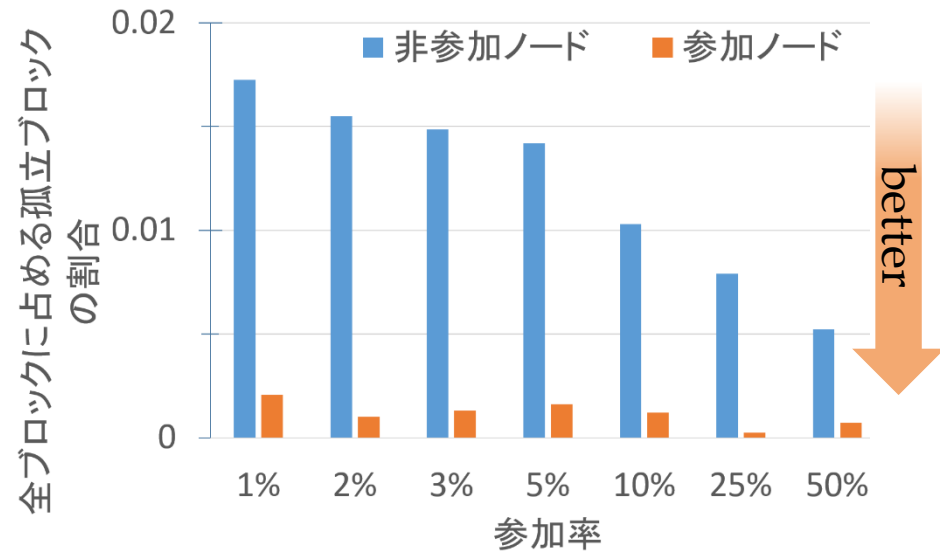
リレーネットワーク 効果推定

[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



セキュリティの研究

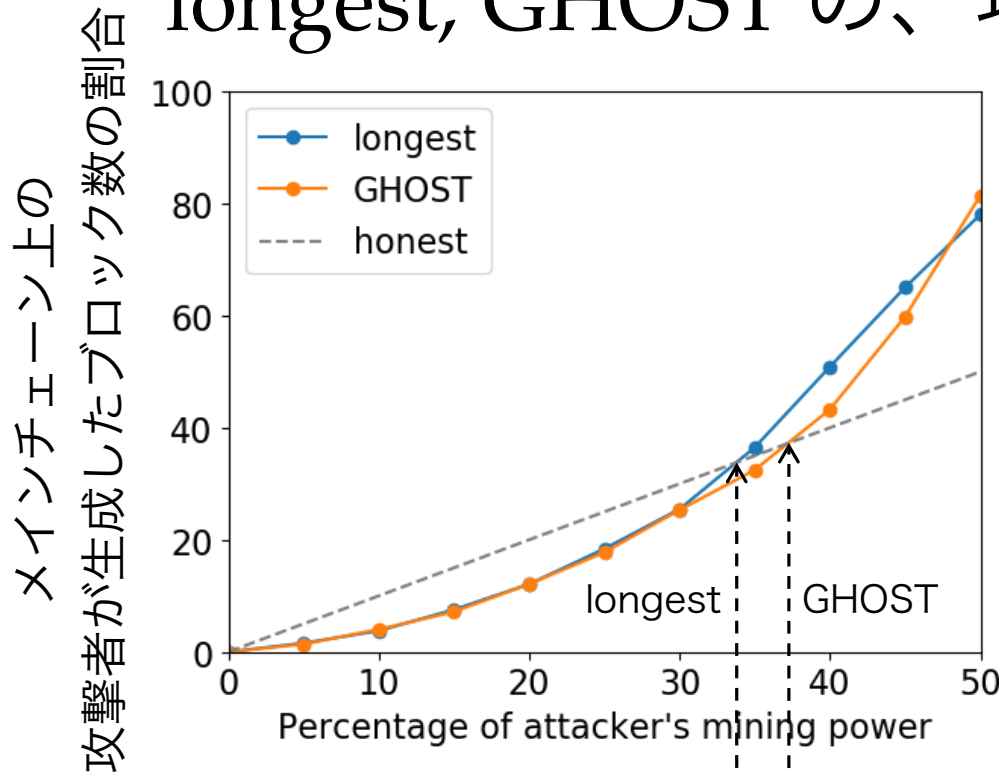
- 性能
- ツール
- セキュリティ
- 公平性
- 分権化

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]

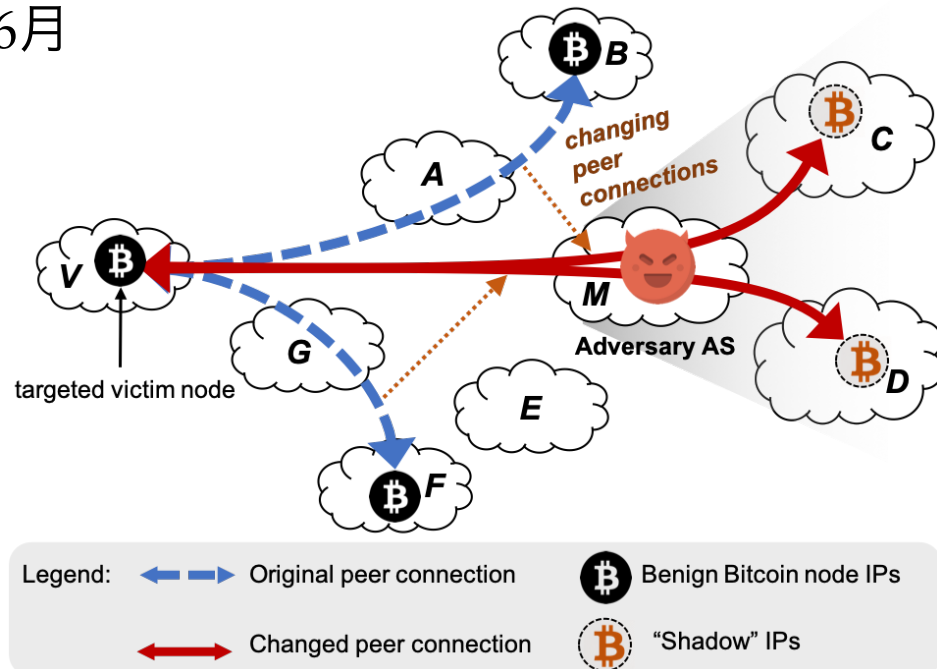
- Erebus 攻撃 (IEEE S&P 2020)
 - ネットワーク分割攻撃 → 様々な使いみち
 - AS を制御する攻撃者がノードを攻撃。
対象ノードを攻撃者のノードに多く接続させる。

- 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？

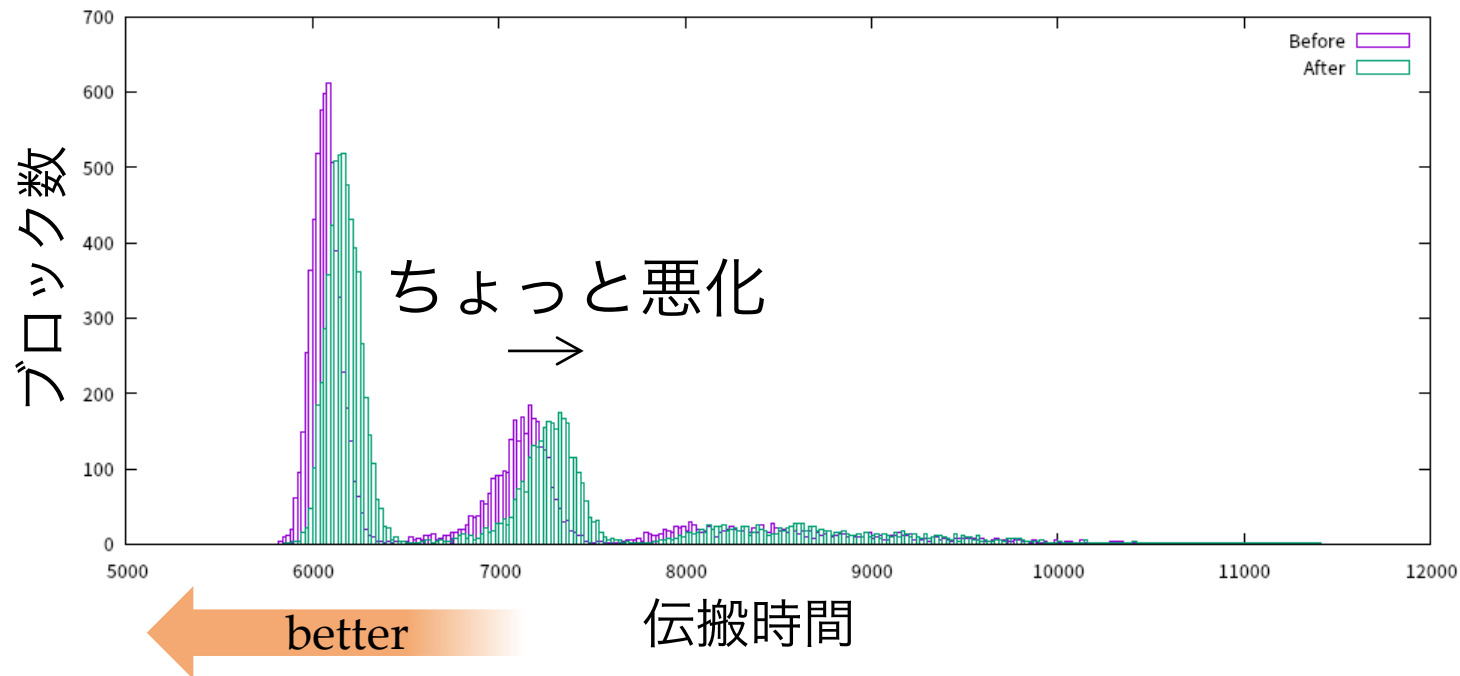


Erebus 攻撃対策の影響推定

[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



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

32 / 39

[神田 2020a]
[Kanda 2020b]

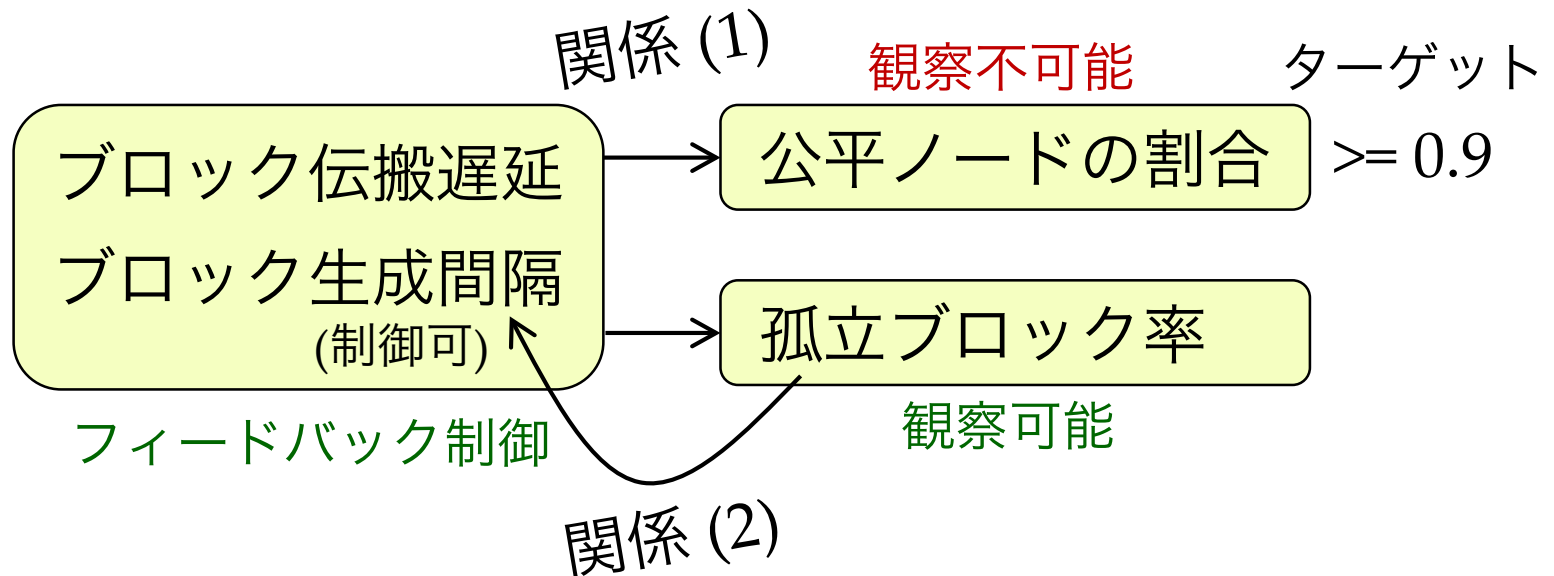
- 公平とは
 - マイニング成功率がハッシュレート (計算能力) に比例
 - ...しかし、伝搬遅延によりブロックの受信が遅れると、その分、マイニングに費やせる時間が減る → 不公平
 - Ethereum なら、
ブロック間隔 13秒前後 – 伝搬遅延が実質マイニング時間
- 既存の公平性 [Cromon 2016] ← 雑すぎる
 - 90% のノードが一瞬でもマイニングできれば公平
- 提案： (X, ε) 公平性
 - 充分長いブロックチェーンに対して、
割合 X のノードが不公平を被る確率 ε 以下。
 - 今回、 $X = 0.9, \varepsilon = 0.01$ 。

ノード間の公平性指標と ブロック生成間隔調整

33 / 39

[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。



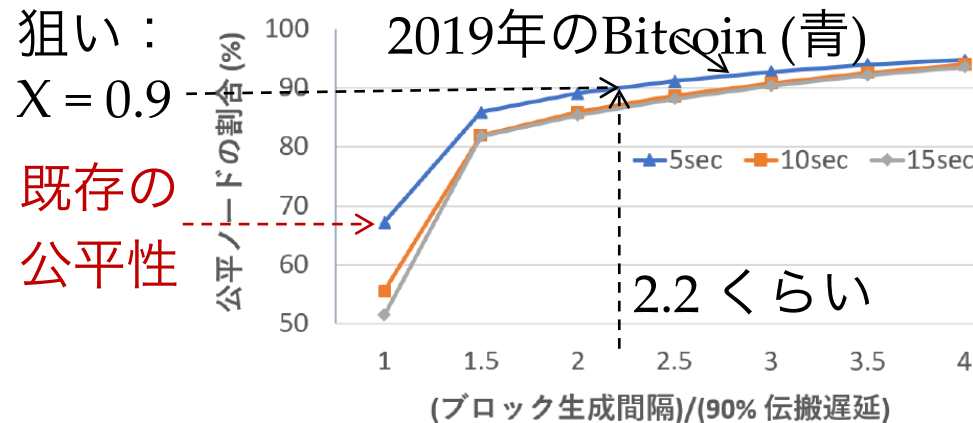
ノード間の公平性指標と ブロック生成間隔調整

[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]

	$\frac{\text{ブロック生成間隔}}{90\% \text{伝搬遅延}} = 2$	$\frac{\text{ブロック生成間隔}}{90\% \text{伝搬遅延}} = 3$
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

36 / 39

[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： $\text{コイン年齢} / \text{coin age}$ (= 金額 $\times$ 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 $\rightarrow$ 51% 攻撃の危険。
 - 報酬：固定額

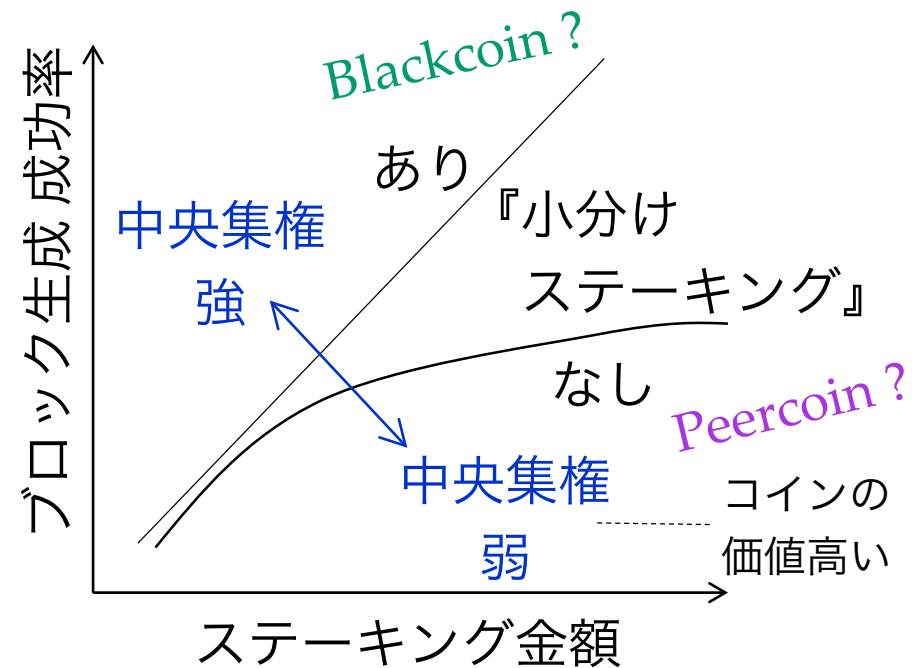
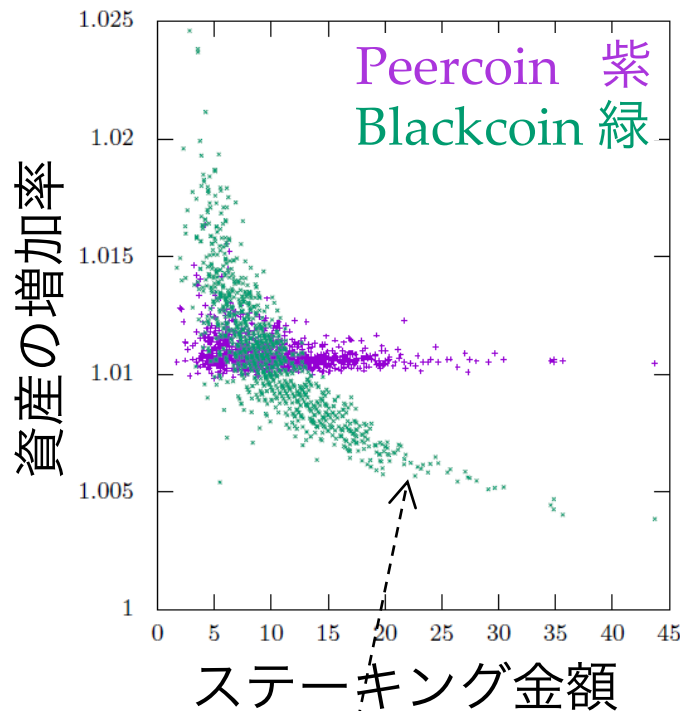
Proof of Stake 各プロトコルの中央集権の度合い

37 / 39

[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

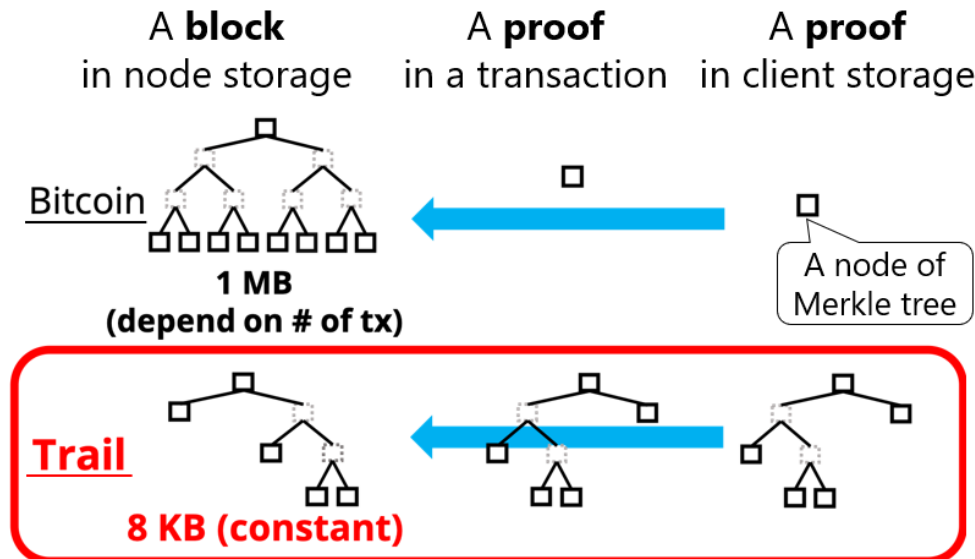
ノードの保持データ量が少ない ブロックチェーン用データ構造 28 / 39

- 大きな台帳データがノード運営の負担で、[Nagayama 2020a]
分権化 / decentralization を妨げている。

- Bitcoin 320 GB, Ethereum 188 GB (2020年 12月)

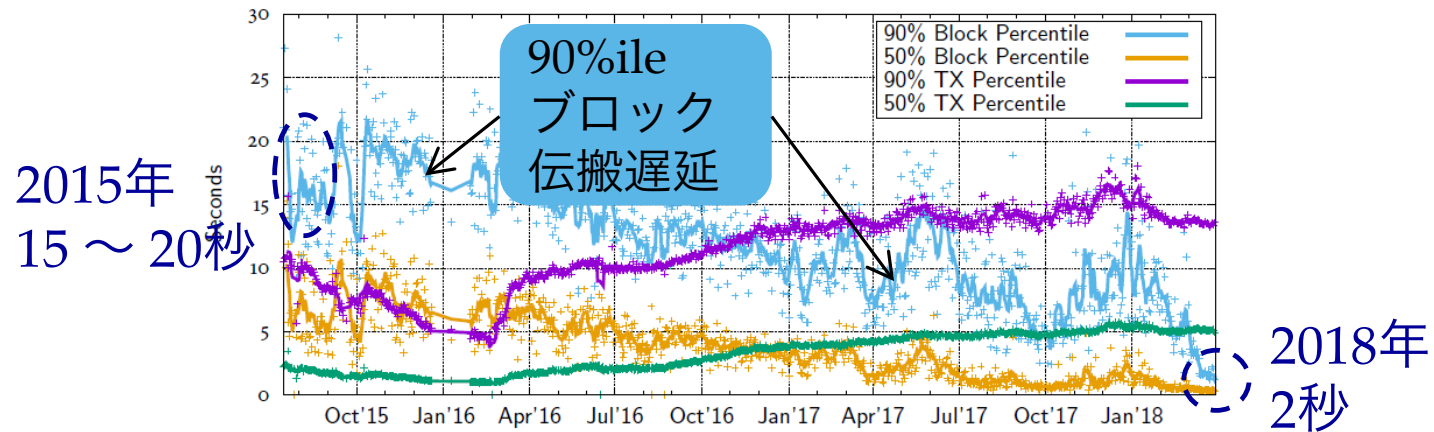
- 提案：

- 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



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...



- 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, 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)

• 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

• 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