京大ミートアップ supported by GMO
2023年 12月 14日(木)

bit.ly/shudo20231214

ブロックチェーンの現在と未来

首藤一幸

京都大学 **学術情報メディアセンター**
京都大学 情報学研究科 **社会情報学専攻**
GMOインターネット(株) 技術顧問

首藤 一幸 (50)

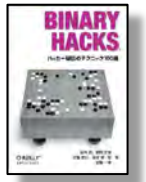
しゅどう　かずゆき

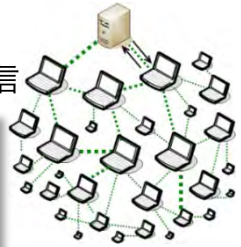
1996　早稲田大学 修士課程
1998　早稲田大学 博士課程
2001　産総研　**国研**
2006　ウタゴエ(株)　**スタートアップ**
2008/12 東工大　**大学**
2022/ 4 京大
2009/ 5 未踏 PM
2023/ 4 未踏アドバンスト PM

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

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





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

大規模分散システム

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 12月

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, …

1万 9千種類あるとか
独自ソフト, geth 使用, Substrate で構築, …

- 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.

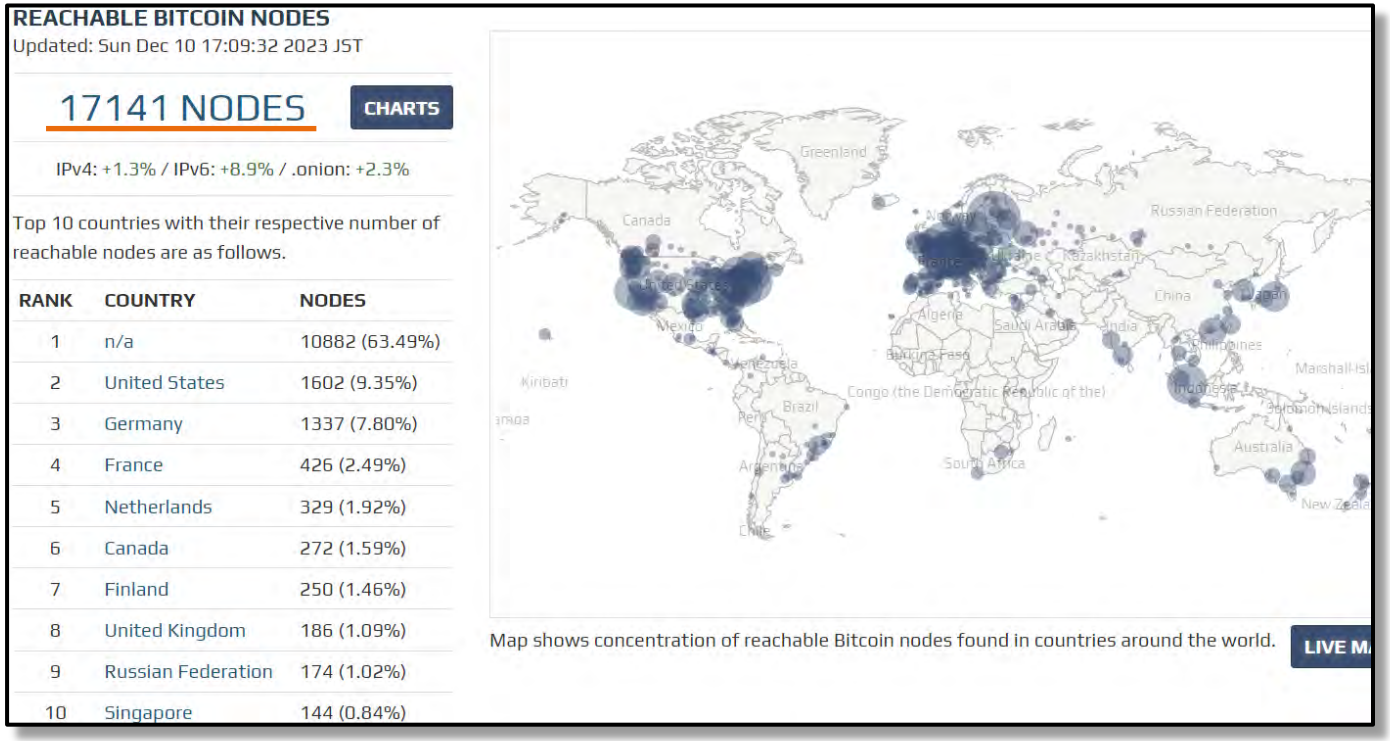
See bitcoin.org for screenshots.

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

多数のコンピュータが支えるBitcoin

- 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



REACHABLE BITCOIN NODES
Updated: Sun Dec 10 17:09:32 2023 JST

17141 NODES CHARTS

IPv4: +1.3% / IPv6: +8.9% / .onion: +2.3%

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

RANK	COUNTRY	NODES
1	n/a	10882 (63.49%)
2	United States	1602 (9.35%)
3	Germany	1337 (7.80%)
4	France	426 (2.49%)
5	Netherlands	329 (1.92%)
6	Canada	272 (1.59%)
7	Finland	250 (1.46%)
8	United Kingdom	186 (1.09%)
9	Russian Federation	174 (1.02%)
10	Singapore	144 (0.84%)

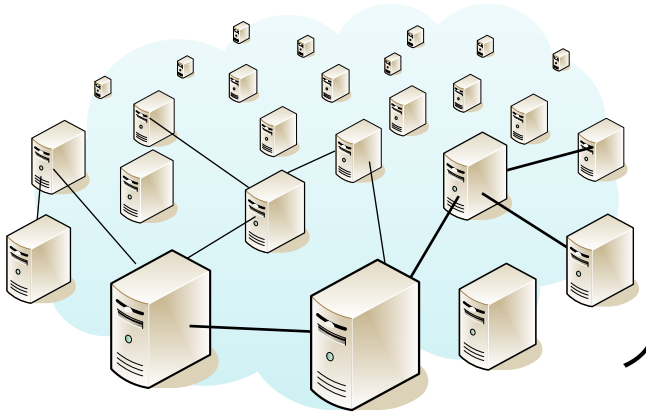
Map shows concentration of reachable Bitcoin nodes found in countries around the world. LIVE M

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

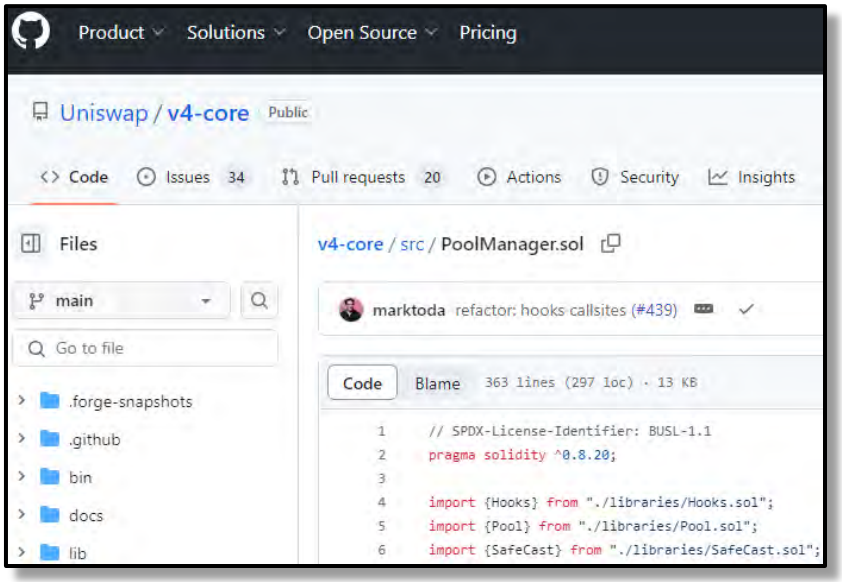
「ブロックチェーン」は特定のデータ構造を指す語なので、
それを嫌って、DLT と呼ぶ人も多い。

様々なイノベーション

- 暗号通貨 Bitcoin (2008)
- スマートコントラクト Ethereum (2014)
- 数多のトークン / コイン ERC-20 仕様 (2015)
- NFT ERC-721 仕様 (2018)
- DeFi Uniswap (2018), …
- DAO 定義 (2014) → The DAO (2016) → …
- Web3 用語 (2014) → 反 Big Tech → 投資の標語

スマートコントラクト

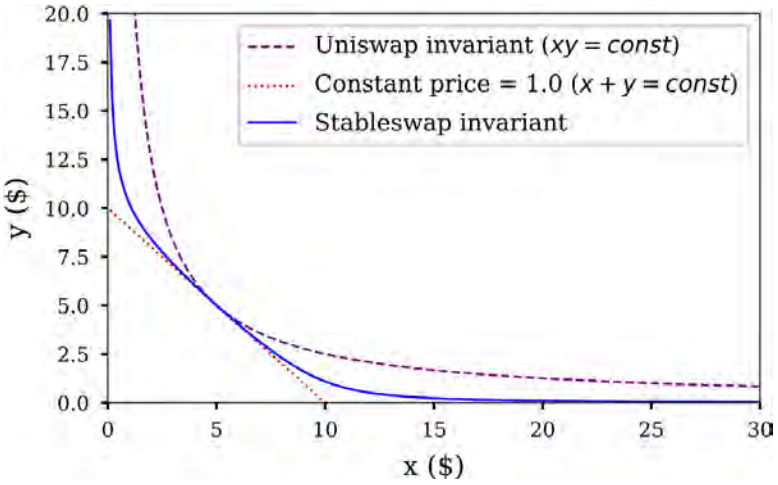
- ブロックチェーン上で動作するプログラム
  - 全ノードが同一の処理をする。無駄っぽいけど、これによって不正を防いでいる
  - Ethereum (2014 ~) が導入
    - Solidity 言語等で記述, EVM で実行
    - おそらく、Bitcoin Script から着想
  - DeFi, DAO など様々なイノベーションの基盤



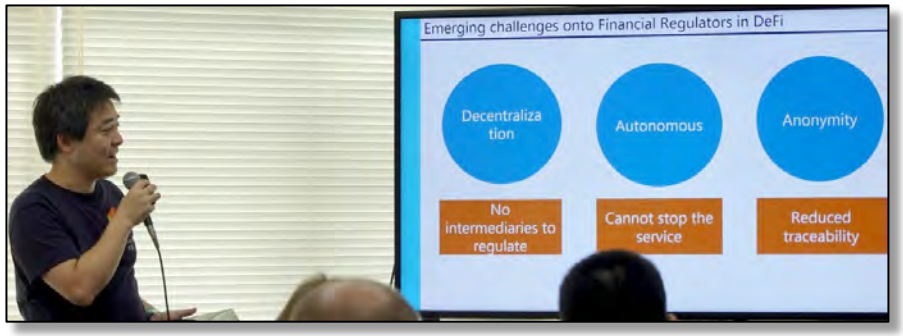
DEX である Uniswap のソースコード in Solidity 言語

DeFi (Decentralized Finance) / 分散型金融

- スマートコントラクトを用いて
  様々な金融サービスを実現する試み
  - 取引所 (両替), 証券, 保険, デリバティブ, 賃借 (銀行), …
- 代表例：DEX / 分散型取引所 Uniswap 等
  - スマートコントラクトが自動で両替



AMM (Automated Market Maker) の数式



金融庁（当時）三輪さんの講演
2019/10/10(木)

DAO (Decentralized Autonomous Organization)

- Ethereum 創設者の 1人 Vitalik Buterin が提唱
  - 2014年 5月のブログ "DAOs, DACs, DAs and More: An Incomplete Terminology Guide"
  - コンピュータによる自動運営組織 (が人間を使う)

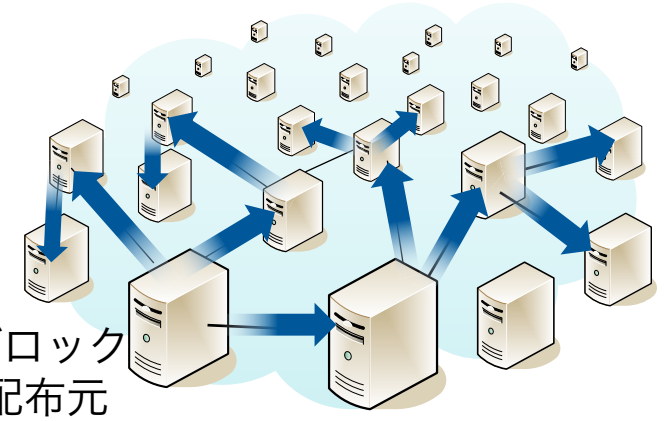
- 理想
  - コンピュータ**プログラムが運営**する組織
    - LLM に「目的」を与えたら、けっこうできちゃいそう。さらに「センサ」と「アクチュエータ」を与えて、うまいこと実世界（めいた場所）で学習させたら、汎用人工知能 (AGI) に？

- 今日
  - 株式の代わりに、**特別なトークン（コイン）の持ち分に応じて、意思決定**していく組織

スケーラビリティ（性能）問題

- 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**

- 性能向上へのアプローチ
  - base layer (ブロックチェーン自体) の改善
    - ブロック伝搬の高速化 by 首藤研 ⟶
    - sharding
    - …
  - Layer 2
    - …の payment protocol　- 例: Lightning Network
    - rollup　- ブロックチェーン外で処理



ノード (サーバ) のネットワーク

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

相互に影響

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

研究手段を提供

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

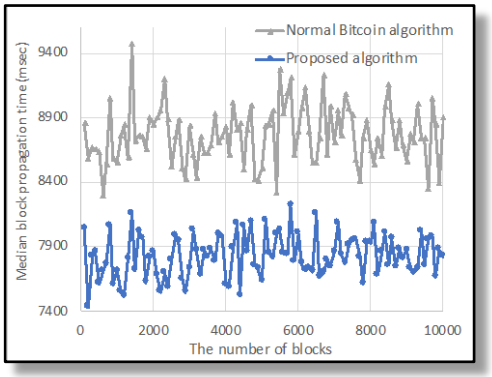
公平性指標と向上手法 [Kanda 2020c]他

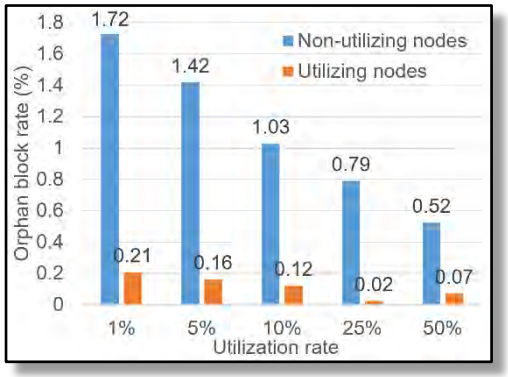
Ethereum 開発者会議 (Devcon 5) での発表 [Nagayama 2019]

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：

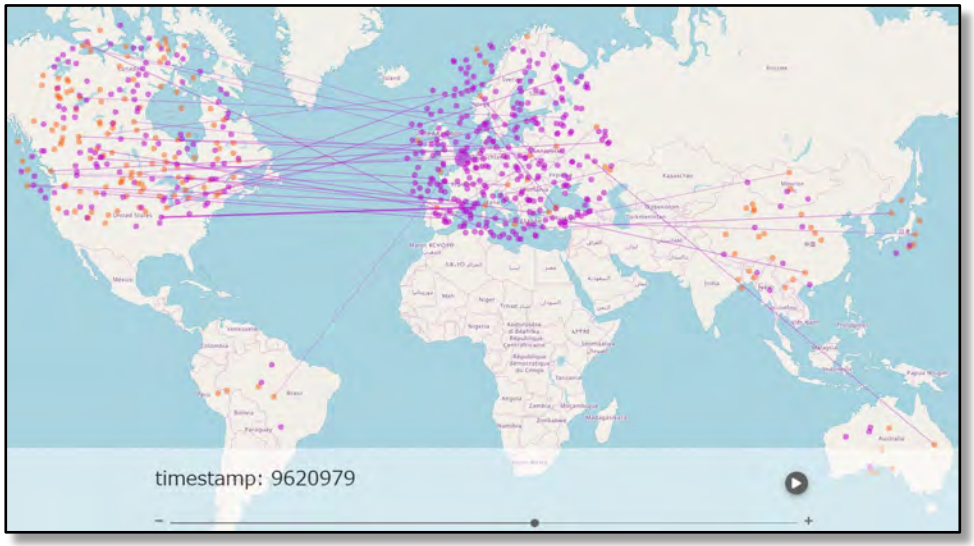




隣接ノード選択　リレーネットワーク 効果推定

シミュレータ SimBlock

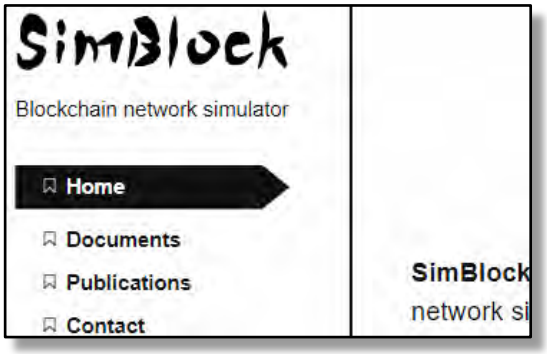
[青木 2019a] [Aoki 2019b] [Banno 2019] [Shudo 2019]



Visualizer

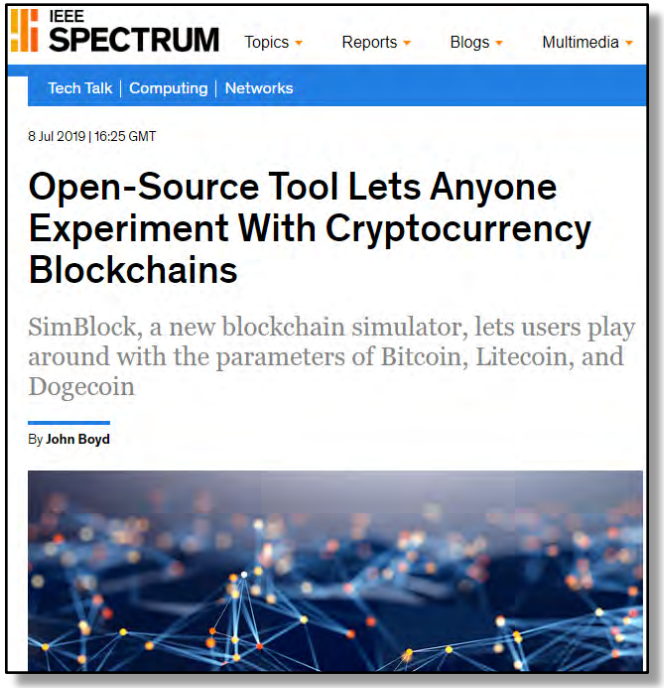
縮小 Bitcoin ネットワーク,
600 ノード

ウェブ
サイト



IEEE ICBC 2019 デモ,
ソウル, 2019年 5月

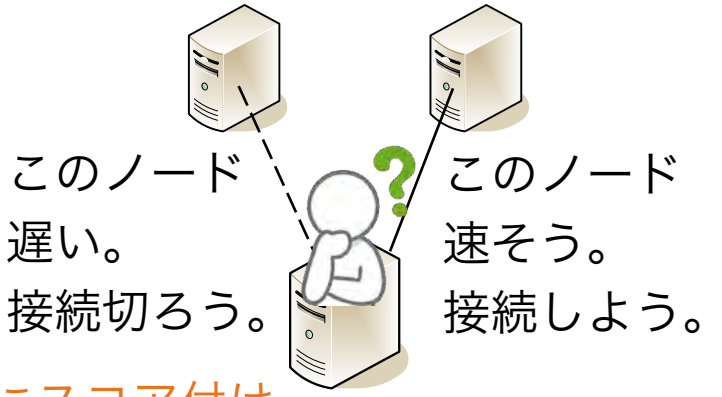
IEEE Spectrum
記事



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
    - 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

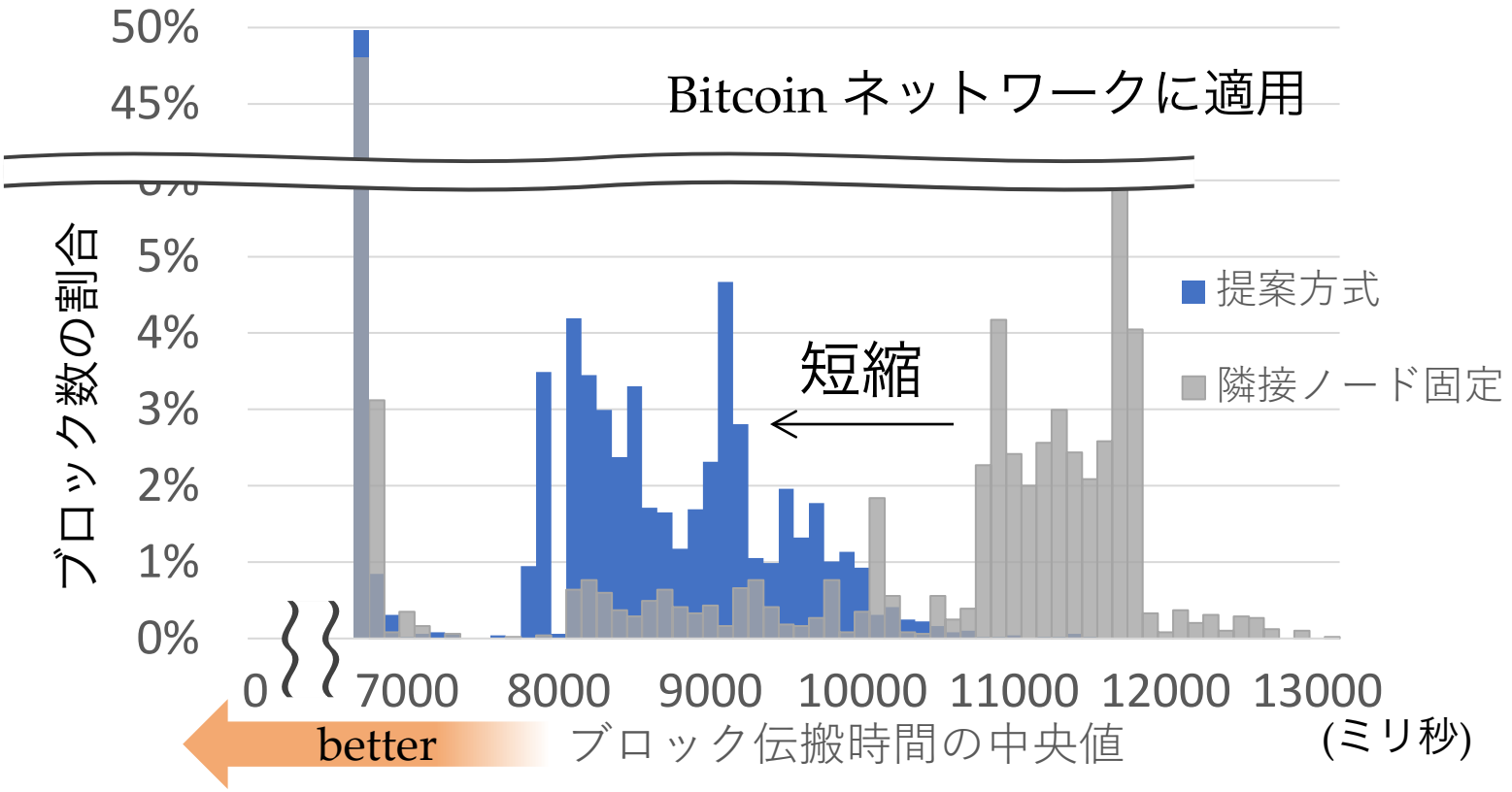


- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

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

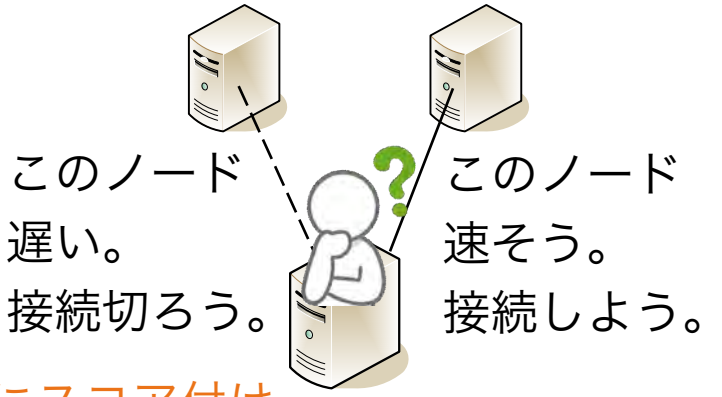


- 注：2015年のインターネットを対象として実験

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

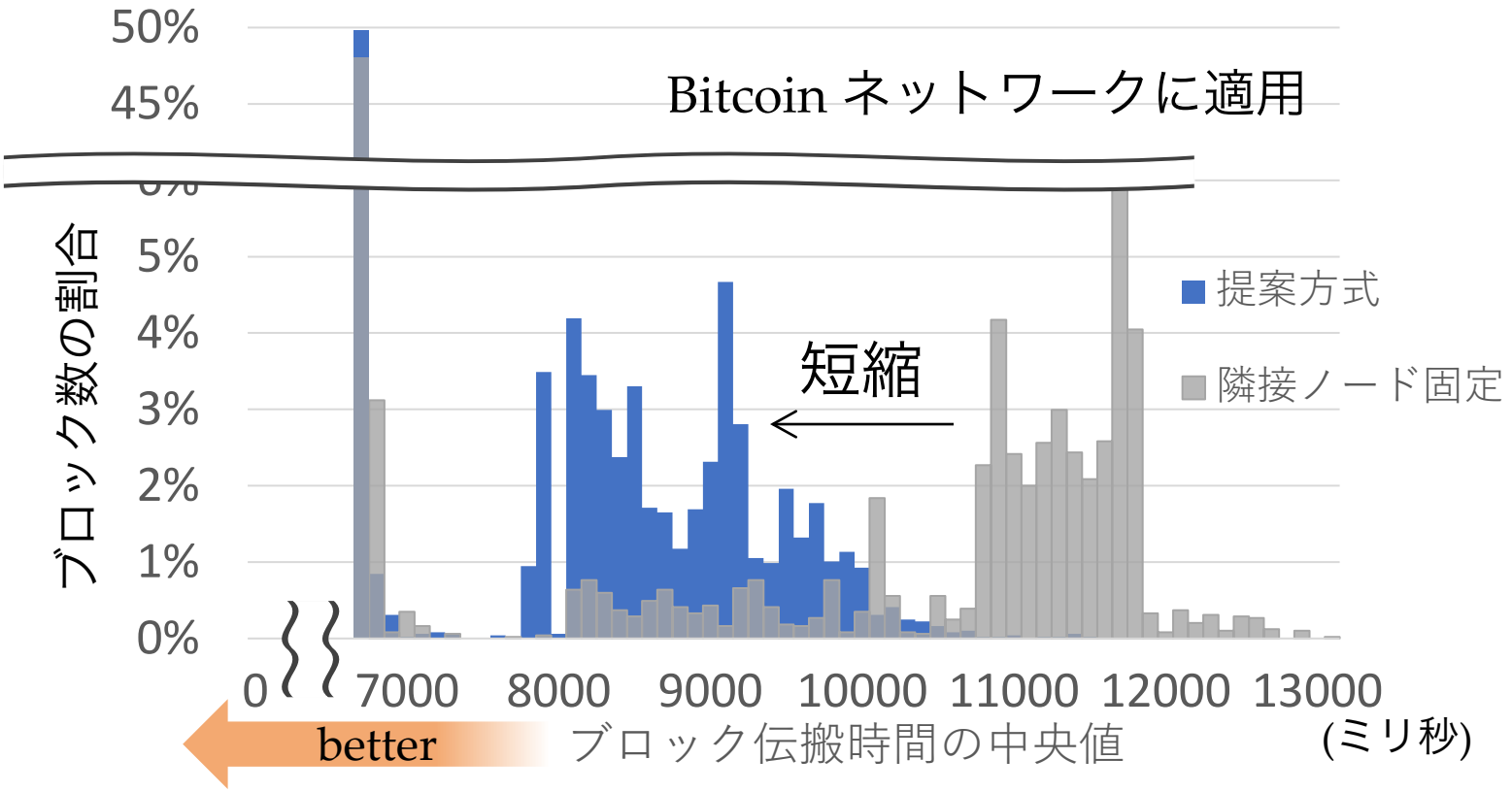


- 手法
  - ブロックを配信してくれた相手ノードすべてにスコア付け
    - スコア = (ブロック配信時刻 – 生成時刻) の指数重み付き平均値
  - 10 ブロック受信するごとに隣接ノードを選択し直す
    - ただし、新しいノードとつながるために、K ノードは知っているノード群からランダムに選ぶ
    - 予備実験の結果：K = 1, P (伝搬時間 最新値の重み) = 0.3

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

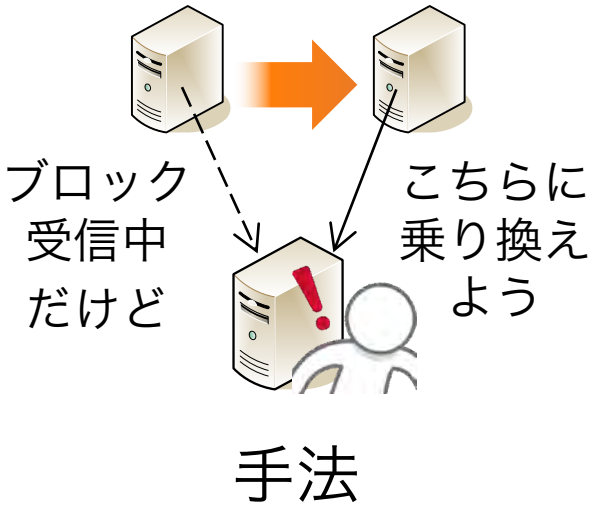


- 注：2015年のインターネットを対象として実験

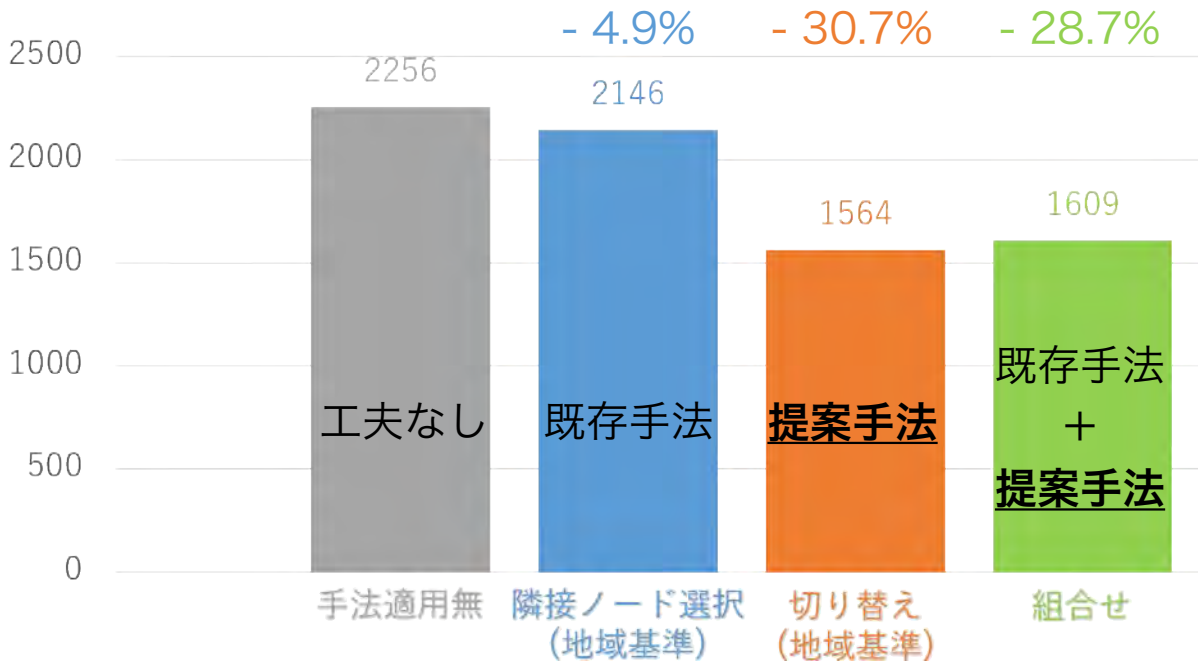
ブロック送信元ノードの切り替え

[櫻井 2022a] [Sakurai 2023a]

- ブロック受信中であっても、
  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

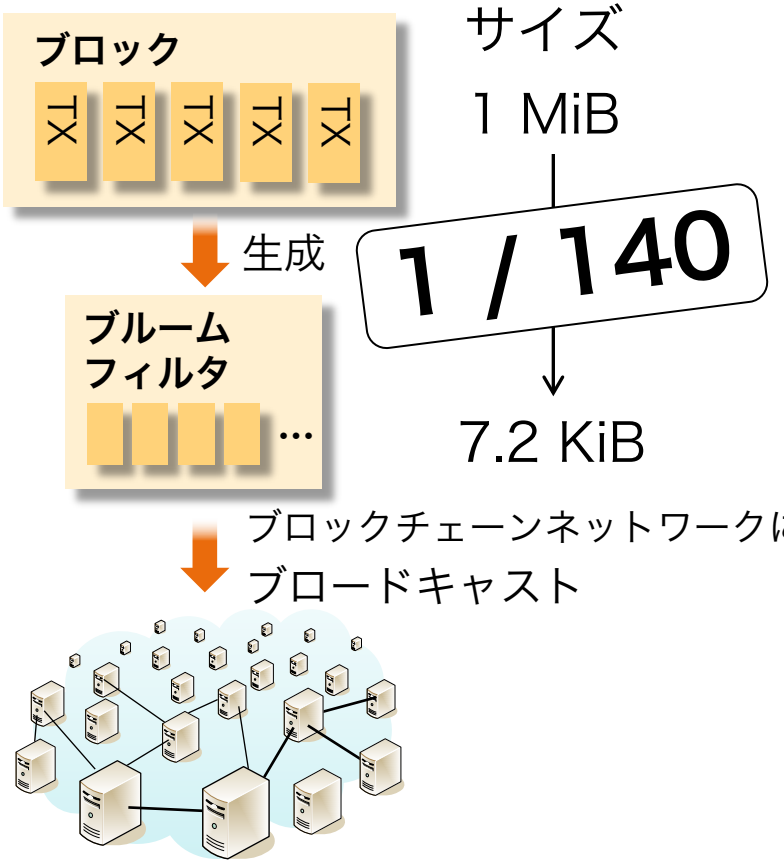


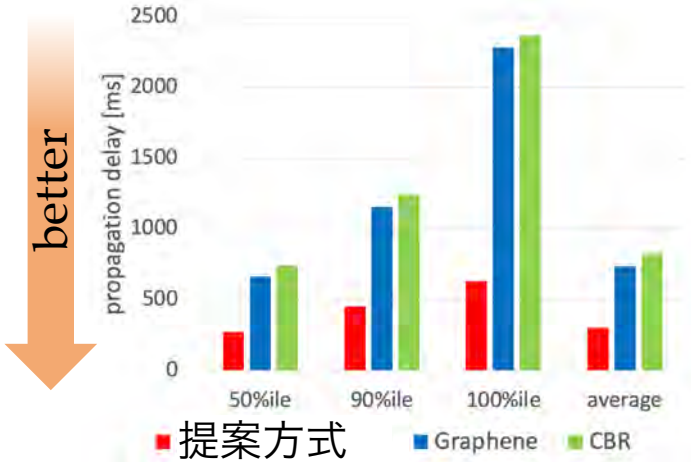
90% のノードにブロックが行き渡るまでの時間

ブロック生成通知

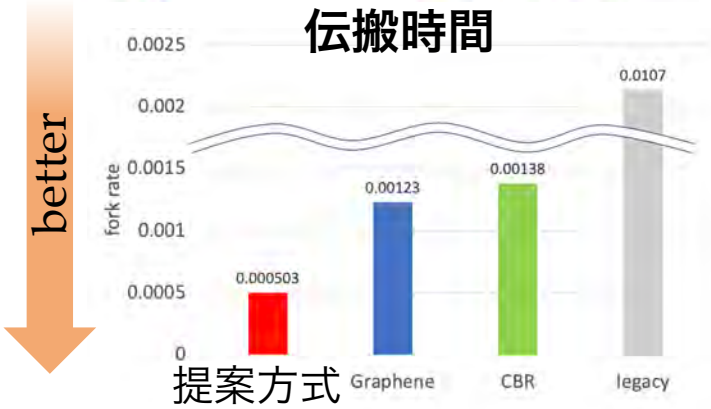
[長谷川 2023a] [Hasegawa 2023b]

- 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。





伝搬時間

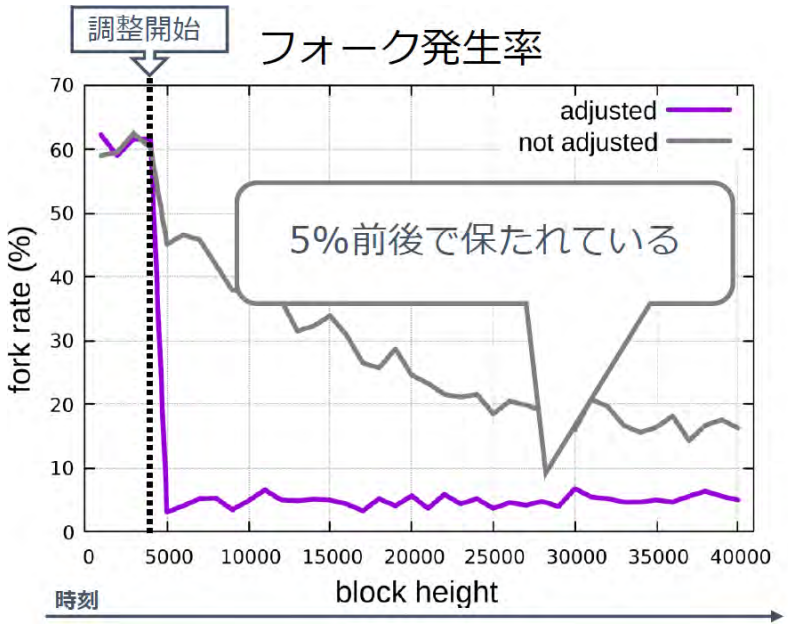


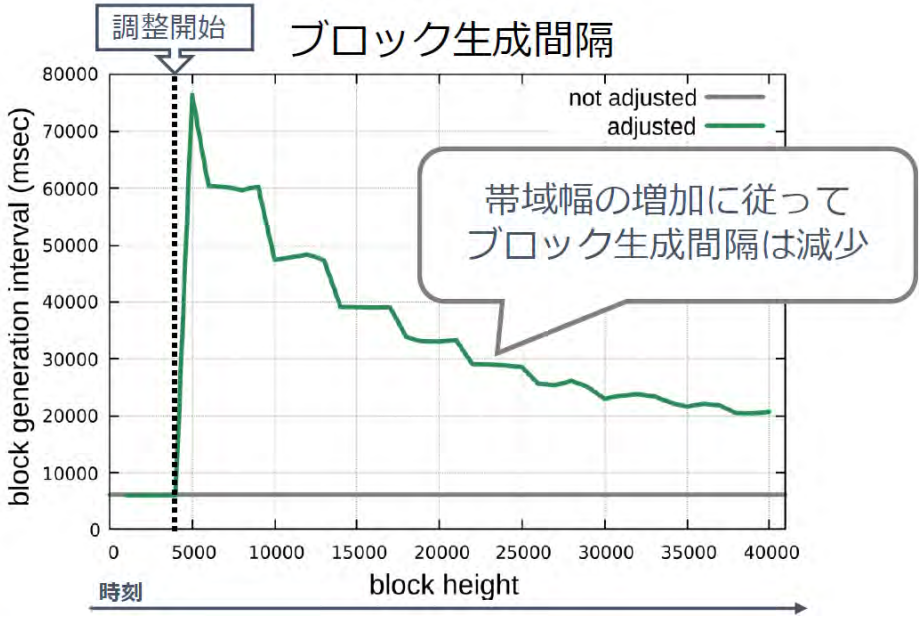
フォーク発生率（セキュリティの指標）

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。

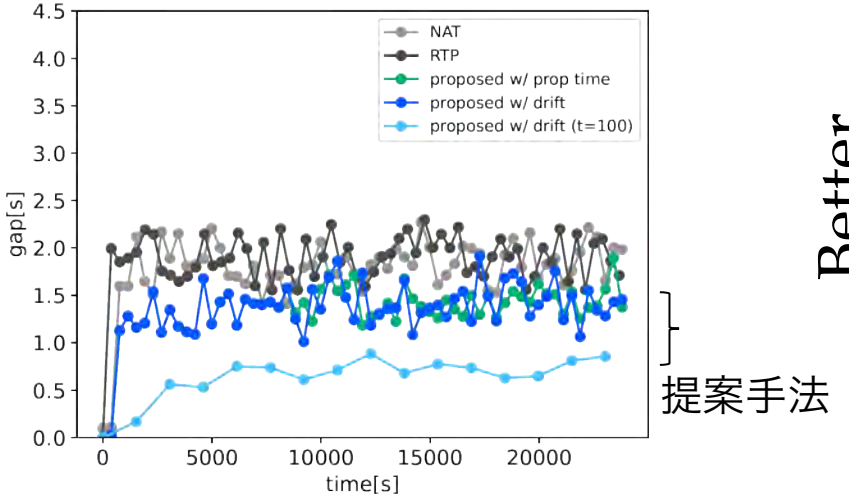




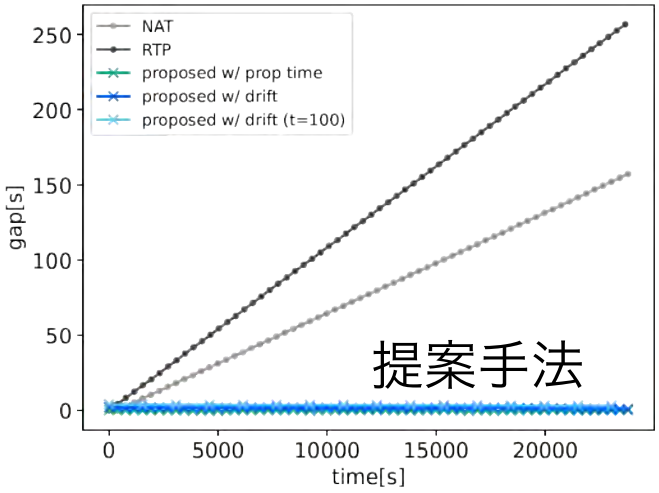
ノード群による 非集中的な 時計合わせ

[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



最早ノードと最遅ノードの差



実世界の時計との差

個人を empower するトラストレス

- ブロックチェーン周辺の 様々なイノベーション
  - 暗号通貨 Bitcoin (2008)
  - スマートコントラクト Ethereum (2014)
  - 数多のトークン / コイン ERC-20 仕様 (2015)
  - NFT ERC-721 仕様 (2018)
  - DeFi Uniswap (2018)
  - DAO 定義 (2014) → The DAO (2016) → …
  - Web3 用語 (2014) → 反 Big Tech → 投資の標語
- Bitcoin が、もし、トラストレスでなかったら？ ※
  - Satoshi Nakamoto が管理・発行するただの電子マネーだったら、誰も買わなかっただろう。
  - トラストレスという性質が、国や大組織にしかできなかったことを個人にまで開放した。

※“トラストレスのメカニズム”, 情報処理, 2023年 1月号